MASTER'S DEGREE THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

Title: Shimura varieties and Gross-Zagier formulae

Author: Armando Gutiérrez Terradillos

Advisor: Victor Rotger

Department: Applied Mathematics

Academic year: 2018-2019

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

UNIVERSITAT POLITÈCNICA DE CATALUNYA

MASTER THESIS:

SHIMURA VARIETIES AND GROSS-ZAGIER FORMULAE

Armando Gutiérrez Terradillos

Supervised by:
Victor Rotger

A mi madre, por su paciencia.

Introduction

An important problem in modern number theory is to understand the behaviour of $L-$functions. Those functions arise as a generalization of the Riemman $\zeta-$function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Apart from their analytic significance, $L-$functions are analytic objects that give information about number theoretic objects. An example of this relation is the Birch and Swinnerton-Dyer conjecture (BSD), that says

"The rank of an elliptic curve E is the order of the zero

of $L(E,s)$ at $s=1$ with L the Hasse-Weil L-function."

To understand the behaviour of those functions, mathematicians have been researching on how to obtain expressions of $L-$functions, hope to find how is their general structure. In this dissertation we study the Gross-Zagier formulae, [8], expressions of $L-$functions in terms of Shimura varieties. A few years later after Gross's paper, the work of Gross and Zagier [10] (1986) combined with the work of Kolyvagin (1989) allows us to prove a restricted case of the BSD conjecture.

A very important part in the work of Gross-Zagier formulae was the introduction of the theory of Shimura varieties. Those objects were introduced by Goro Shimura in some papers during the 1960's. Shimura worked with quotients of hermitian symmetric domains with the objective of generalizing the reciprocity law of complex multiplication theory. From a less technical point of view, we can understand Shimura varieties as the generalization of modular curves. This construction also has good behaviour respect the moduli point of view, since these varieties parametrize certain families of abelian varieties; the higher dimensional version of elliptic curves. Apart from their importance and mathematical wealth per se, Shimura varieties have been used to compute values of $L-$functions, to solve problems in arithmetic geometry, and as a natural realm of examples in the Langlands program.

The relation between Shimura varieties and number theory arises from functions that are naturally defined over a Shimura variety. Classically, modular forms are functions defined over a modular curve, we use those functions because they have information about number theoretical questions, and these have allowed us to prove a lot of important result in number theory in the last century. We can define analogous functions over Shimura varieties, these functions can translate geometric information of our Shimura variety to solve a certain problem in number theory. In the study of those maps, automorphic forms theory plays an important role, then along this dissertation, an introduction to this theory is explained.

This relation is not an artificial construction to solve only one problem. We can see their natural connection in the proof of the Gross-Zagier formulae, where Gross uses the theory of Shimura

varieties to find an explicit realization of the Jacquet-Langlands correspondence. This is motiveted because this correspondence allows us to translate a modular forms problem to a quaternionic modular forms problem. In this case the latter problem is easier due to the fact that the quaternionic Shimura curve that Gross constructs is totally definite, i.e, this curve is a finite set of points, and therefore has an easier arithmetic structure.
In the original paper [8], Gross omits the geometric point of view, actually he constructs an algebraic object obtaining desired properties of about embeddings of quadratic orders on quaternion orders; this algebraic object is in fact a Shimura variety. Actually, this paper can be read without any idea of what is a Shimura variety. The naturalness of the construction in this paper shows that this relation goes further than a sporadic use, Gross-Zagier formulae can be seen as a case in to a bigger theory; this point of view is explained in the chapter 3, section 10.

This dissertation is divided into 3 parts. In the first chapter we introduce needed concepts about algebra and complex geometry. A lot of results that are there are crucial to prove important properties in the other two chapters; as the Baily-Borel's theorem, which allows us to define an algebraic structure for Shimura varieties. Even thought this chapter contains important results, we prove few of them, due to the fact that the topic of this dissertation is the arithmetic enclosed by certain geometric objects (Shimura varieties). Then the role of this chapter is to be a library of theorems.

The second chapter starts explaining the basic theory about the ring of adéles, a global concept which contains all the local data of a ring. This ring plays a crucial role in the construction of Shimura varieties, providing us important theorems as *strong approximation theorem*. After that, we give the definition of what is a Shimura variety (connected and non-connected), and then we prove basic properties about them. With the help of the adele's theory we prove that we can express every Shimura variety as the following double quotient

$$G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$$

Since Shimura varieties are the generalization of modular curves, it would be expected that these varieties would parametrize some family of "generalizations" of elliptic curves. Indeed, this expectation is fullfilled; we construct the *Siegel modular variety*, *Hodge type variety* and *PEL variety*, which define three moduli spaces of abelian varieties. The construction of the Siegel modular variety is based on the action of the symplectic group Sp_n over a symplectic vector space. To define the other two varieties, we restrict this construction in two ways. With these restrictions, we can find elements, as Hodge structures, which define more restricted moduli spaces. Instead of being an incidental fact, being a moduli space can help us to obtain some results, carrying problems about our Shimura variety to a moduli problem, and solving there the problem. An example of this, is the work of Kolyvagin (1989), where he studies Heegner points of $X_0(N)$, the moduli space of (E, C) with E elliptic curve and $C < E$ subgroup of order N. Using the information given by those points, Kolyvagin finds relations between the $K-$rational points of the elliptic curve E and values of the $L-$function.

Due to Baily-Borel's theorem, Shimura varieties are in fact algebraic varieties. In the next section we study the canonical model of a Shimura variety, an accurate way to define a Shimura variety as an algebraic variety. The terminology is due to the fact that we can always define the equations of our Shimura curve over the *reflex field*, which provides a canonical way to define every Shimura variety in terms of its automorphisms. This field is defined as the fixed field of the $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ which fix certain cocharacters, i.e

$$E(G, D) = Fix\{\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}) : \ c_D^\sigma \cong c_D \in \mathfrak{C}(\overline{\mathbb{Q}})\}$$

We define this concept with the help of the Artin reciprocity, which sends elements of the adele ring to the automorphisms group. This allows us to define the notion of what is a canonical model in a purely abstract way, without involving any polynomial or tedious tool.

After this section we study a specific type of Shimura varieties; quaternionic Shimura varieties. Those varieties are constructed using B^*, the multiplicative algebraic group of a quaternion algebra. We describe the construction of a quaternionic Shimura variety for the definite and indefinite case, obtaining their quotient expressions

$$X = \Gamma_0^B(\mathfrak{N}) \setminus \mathcal{H}^r \quad \textit{and} \quad Y = B^* \setminus \mathbb{P}^1 \times B(\mathbb{A}_f)^*/\hat{R}$$

Afterwards, using basic definitions about automorphic forms, we define the natural functions on quaternionic varieties. We explain their behavior, and we give necessary propositions to state the Jacquet-Langlands correspondence, which gives the existence of an injective map between quaternionic modular forms of two quaternion algebras.

The last two sections are developed to define the Gross-Zagier curve. We analyze this curve along the last section, applying the theory of Shimura varieties explained in this dissertation. This curve is a quaternionic definite Shimura curve, and is the curve which we use to find expressions of the $L-$functions in the next chapter. This construction is a beautifull example of how arithmetic geometry works. We start with algebraic objects, as *optimal embeddings*, we use their properties to construct a geometric object as

$$X = B^* \setminus Hom(K, B) \times \hat{B}^*/\hat{R}$$

and we use geometric objects or tools to solve our problem geometrically.

Using properties of Shimura varieties we obtain other expressions of this Shimura curve and its special points. With the help of the correspondences between points of X, elliptic curves and ideals, along this section we translate properties of Shimura curves to properties of optimal embeddings. In this section we also study the functions defined on X, obtaining different ways to understand $Pic(X)$. All this theory creates a geometry in terms of algebraic objects with the aim of solving an arithmetic problem.

The third chapter begins explaining the properties of Brandt matrices, algebraic objects that arise as coefficients of a modular form which contains information about a quaternion algebra;

$$j_{ij} = \frac{1}{2w_j} \sum_{b \in M_{ij}} e^{2\pi i (n(b)/n(M_{ij}))\tau} = \sum_{m \geq 0} B_{ij}(m) q^m$$

These matrices act like a glue in the rest of the chapter. They help us to obtain the realization of the Jacquet-Langlands correspondence between $X = X^B$ and $X^{M_2(\mathbb{Q})}$. We use their properties to obtain how the Hecke operator acts in the space of modular forms of X_B.
After studying these matrices, we give some properties about supersingular elliptic curves. These curves are related to our problem because their endomorphism ring is an order of a quaternion algebra. We exploit this relation to obtain a bijective correspondence between points of X and supersingular elliptic curve. This allows us to use some from the theory of elliptic curves to solve problems about points of X.

In the third section we state the main result: Given the $L-$function

$$L(f, A, s) = \sum_{\substack{m=1 \\ (m,N)=1}}^{\infty} \frac{\epsilon(m)}{m^{2s-1}} \sum_{m=1}^{\infty} \frac{a_m r_A(m)}{m^s}$$

we can express its special value as

$$L(f, A, 1) = \frac{(f, G_A)}{\sqrt{D}}$$

with G_A an expression involving special points of X.
Apparently, this is an analytic problem, and in fact, with the help of the Rankin's method, we simplify this expression. This method gives us an expressions in terms of the trace, therefore in the next section we compute the trace, giving a more manipulable expression.
The fifth section could be the most important part of this chapter. This is because in this part we give the explicit realization of the Jacquet-Langlands correspondence, called the *Eichler correspondence*. This relation helps us to solve some problems relating modular forms, just because we can translate a modular forms problem to a problem of $Pic(X)$, the set of line bundles of a finite set of points.

$$\begin{aligned} \phi :\ Pic(X) \otimes_{\mathbb{T}} Pic(X)^\vee \longrightarrow &\quad M \\ \phi(e, e^\vee) \longrightarrow & \frac{deg\ e \cdot deg\ e^\vee}{2} + \sum_{m \geq 1} \langle t_m e, e^\vee \rangle q^m \end{aligned}$$

In the following chapter, with the help of this correspondence and using tools inherited from the "*elliptic curves-ideals-points of* X correspondence", we express this $L-$function in terms of special points of X, obtaining the desired result.

In the next three sections we give expressions of other $L-$functions as

$$L(f,\chi,s) = \sum_{A \in Pic(O)} \chi(A) L(f,A,s) \quad or \quad L(f,\chi=1,1) = L(f,1)L(f\otimes\epsilon,1)$$

The last $L-$function has a crucial importance in number theory, and this is the inspiration of the next two sections. Using Shimura's ideas about modular forms of semi entire weight, we reinterpret this result in terms of modular forms of weight 3/2, obtaining a correspondence between Hecke modules, as with the Eichler correspondence. Doing a reasoning similar to the main result proof, we obtain the Waldspurger's formula

$$L(f,1)L(f\otimes\epsilon,1) = \frac{(f,f)}{\sqrt{D}} \frac{m_D^2}{\langle e_f, e_f \rangle}$$

In the last section we give a higher point of view of these results, explaining the Gross-Zagier formulae as a fraction. Inspired by the congruences between modular forms, the study of this sort of fractions arises due to the attemps to understand how the Peterson inner product varies when we apply the Jacquet-Langlands correspondence, i.e, how is the behaviour of these fractions

$$\frac{(f,f)}{(f_B,f_B)}$$

This point of view allows us to study this theory as a part of other bigger theory, where we have tools from Galois representation, Shimura varieties, modular forms, and $L-$functions. Anyway, this last section is an additional section, where we do not explain in detail any result, giving only the line of thought of this area of mathematics nowadays.

I would like to write the acknowledgements in my mother tongue, spanish.

Me gustaría dar las gracias a Victor Rotger, gracias a el he aprendido mas teoría de números de la que sabía que existía antes de llegar, y he conseguido comprender (creo) conceptos profundos y complicados. Gracias a el este año he aprendido más matemáticas que nunca. También me gustaría darle las gracias por la ayuda que me ha dado para buscar un proyecto de doctorado, gracias a su ayuda me he iniciado en el mundo de la investigación matemática, en la que espero continuar muchos años.

También me gustaría agradecer la ayuda y apoyo del grupo de estudio de teoría de números; O. Rivero, F. Gatti, M. Roset, V. Hernandez y M.F. Alsina. Os doy las gracias por aclararme tantas

dudas, ayudarme a comprender todo esto mucho mejor, y por supuesto por los buenos momentos a nivel personal, tanto haciendo matemáticas como hablando, he disfrutado mucho de vuestra compañía. Espero que pronto podamos colaborar juntos.

Contents

Chapter 1

Background

As is known, number theory is a field of mathematics which encompass a lot of theory. In this chapter, we have written ideas and theorems that will be necessaries along the dissertation. Sections 1 and 2 are about the arithmetic of quadratic fields and quaternion algebras. These objects are closely related to optimal embeddings by Gauss theory. This will be a crucial idea in the Gross-Zagier formulae proof, because we will obtain tools to solve our problem inherited from the theory of quadratic fields. The third section is about the geometric background that we will need to define what is a Shimura variety. In this last section, we will study Lie groups, algebraic groups, and Hermitian symmetric domains with the aim to give an algebraic structure to the quotient expression which defines modular curves and Shimura varieties (via Borel's Theorem).

1.1 Quadratic fields

Let K be a quadratic field, then we can express it as $K = \mathbb{Q}(\sqrt{\gamma})$. By the theory of quadratic forms, there exists a bijection:

$$\left\{\begin{matrix} \textit{Binary quadratic forms} \\ \textit{of discriminant } d < 0 \end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix} \textit{Ideals of the ring of integers} \\ \textit{of a field with discriminant } d \end{matrix}\right\}$$

Proposition 1.1.1. *Let $K = \mathbb{Q}(\sqrt{\gamma})$ be a quadratic field*

1. $O_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{\gamma}$ *if* $\gamma \equiv 2, 3\ (4)$.
2. $O_K = \mathbb{Z} \oplus \mathbb{Z}((-1 + \sqrt{\gamma})/2)$ *if* $\gamma \equiv 1\ (4)$.

Proof. If we have $\alpha = r + s\sqrt{\gamma}$ with $r, s \in \mathbb{Q}$. Using the norm, $\alpha \in O_K$ if and only if $r^2 - s^2\gamma \in \mathbb{Z}$. If we set $2r = m$, $2s = n$, then $r^2 - \gamma s^2 \in \mathbb{Z}$ implies that $m^2 - dn^2 \equiv 0\ (4)$.

1. If $\gamma \equiv 2, 3\ (4)$, $m^2 - \gamma n^2 \equiv m^2 + 2n^2 \equiv m^2 + n^2\ (4)$. This is congruent to 0 modulo (4) if and only if m and n are even. This is satisfied if and only if $r, s \in \mathbb{Z}$.
2. If $\gamma \equiv 1\ (4)$, we have that $m^2 - \gamma n^2 \equiv m^2 - n^2\ (4)$. $m^2 - n^2 \equiv 0\ (4)$ if and only if m and n are both odd or vice versa. Going back to the first equality, we see that $O_K = \{(m + n\sqrt{\gamma})/2 \ s.t\ m \equiv n\ (2)\}$. Now, we divide $(m + n\sqrt{\gamma})/2$ in two addens

$$(m + n\sqrt{\gamma})/2 = (m + n)/2 + n(-1 + \sqrt{\gamma})/2$$

Using the fact that if $\alpha = (m + n\sqrt{\gamma})/2 \in O_K$, then $m \equiv n\ (2)$. We can observe that $O_K \subseteq \mathbb{Z} \oplus \mathbb{Z}(-1 + \sqrt{\gamma})/2$. The other $\supseteq$ is obvious.

∎

Proposition 1.1.2. *The discriminant $disc(K)$ of a quadratic field $K = \mathbb{Q}(\sqrt{\gamma})$ is given by*

1. $d = disc(K) = 4\gamma$ *if* $\gamma \equiv 2, 3\ (4)$.
2. $d = disc(K) = \gamma$ *if* $\gamma \equiv 1\ (4)$.

Proof. 1. If $\gamma \equiv 2, 3\ (4)$, we have the basis $\{1, \sqrt{\gamma}\} = \{b_1, b_2\}$. We can compute the trace

$$(t(b_i, b_j)) = \begin{pmatrix} 2 & 0 \\ 0 & 2\gamma \end{pmatrix}$$

concluding that $disc(K) = 4\gamma$.

2. If $\gamma \equiv 1\ (4)$, we have the basis $\{1, (-1 + \sqrt{\gamma})/2\} = \{b_1, b_2\}$. We can compute the trace

$$(t(b_i, b_j)) = \begin{pmatrix} 2 & -1 \\ -1 & (1+\gamma)/2 \end{pmatrix}$$

concluding with $disc(K) = \gamma$.

∎

Proposition 1.1.3. *Let p odd*

1. *If $p \not| disc(K)$ and $(\frac{\gamma}{p}) = 1$, then $(p) = PP'$ with $P \neq P'$.*
2. *If $p \not| disc(K)$ and $(\frac{\gamma}{p}) = -1$, then $(p) = P$.*
3. *If $p | disc(K)$, then $(p) = P^2$.*

With $(p), P, P'$ ideals in the ring of integers of K.

Proof. 1. Suppose $(\frac{\gamma}{p}) = 1$, we can find $a \in \mathbb{Z}$ such that $a^2 \equiv \gamma\ (p)$. We can factorize our ideal as $(p) = (p, a + \sqrt{\gamma})(p, a - \sqrt{\gamma})$.
To prove this we have that $(p, a + \sqrt{\gamma})(p, a - \sqrt{\gamma}) = (p)(p, a + \sqrt{\gamma}, a - \sqrt{\gamma}, (a^2 - \gamma)/p)$. And $(p, a + \sqrt{\gamma}, a - \sqrt{\gamma}, (a^2 - \gamma)/p)$ contains p and $2a$. These numbers are relatively prime and we can obtain $\sqrt{\gamma}$ in the same way. This implies that this ideal is O_K. If $(p + \sqrt{\gamma}) = (p - \sqrt{\gamma})$, then these two ideals would contain p and $2a$. This would imply that $(p) = O_K$ and this is a contradiction.

2. If $deg\ P = 1$, then $|O_K/P| = p$. We have an injective map $\mathbb{Z}/p\mathbb{Z} \hookrightarrow O_K/P$. Then every coset of D/P is represented by a integer, due to this map.
Let $a \in \mathbb{Z}$ such that $a \equiv \sqrt{\gamma}\ (P)$, $a^2 \equiv \gamma\ (P)$ and $a^2 \equiv d\ (p)$. This is a contradiction, then $deg\ P = 2$.

3. $(p) = (p, \sqrt{\gamma})^2$. To prove this, we have that $(p, \sqrt{\gamma})^2 = (p)(p, \sqrt{\gamma}, \gamma/p)$. Numbers p and γ/p belongs to the ideal $(p, \sqrt{\gamma}, \gamma/p)$. They are relatively prime so we can conclude that $(p, \sqrt{\gamma}, \gamma/p) = O_K$.

∎

Proposition 1.1.4. *If $\gamma < 0$ and squarefree, then:*

1. $U = \{1, -1, i, -1\}$ *if* $\gamma = -1$.
2. $U = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$ *with* $\omega = (-1 + \sqrt{-3})/2$ *if* $\gamma = -3$.
3. $U = \{1, -1\}$ *if* $\gamma \neq -1, -3$.

Proof. Using the structure of the ring of integers, if $\gamma \equiv 2, 3\ (4)$ we can write any unit as $x + \sqrt{\gamma}y$ with $x, y \in \mathbb{Z}$. If $N(\alpha) = \pm 1$, $x^2 + |\gamma|y^2 = 1$. If $\gamma = -1$, there are 4 possible solutions, $U_{-1} = \{1, -1, i, -i\}$. If $|\gamma| > 1$, $U_\gamma = \{1, -1\}$.
If $\gamma \equiv 1\ (4)$, we can write any unit as $(x + \sqrt{\gamma}y)/2$. If $N(\alpha) = \pm 1$, we have that $x^2 + |\gamma|y^2 = 4$. If $\gamma = -3$, we have that the solutions to this equation are $U_{-3} = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$. If $|\gamma| > 3$, then $U_\gamma = \{1, -1\}$. ∎

Proposition 1.1.5. *Let O be an order in K, $F = [O_K : O]$ is finite and*

$$O = \mathbb{Z} \oplus FO_K$$

F is called the conductor of the order.

To prove this proposition we need an aditional lemma.

Lemma 1.1.6. *Let $A \subset B \subset C$ three free abelian groups of rank r. If $[C : A] = [C : B]$, then $A = B$*

Proof. If we obtain basis of A, B, C, b_1, b_2, b_3 respectively, we can obtain matrices M_1, M_2 such that $b_1 = M_1 b_2$, $b_2 = M_2 b_3$. $[C : A] = |det\ M_1 M_2|$ and $[C : B] = |det\ M_2|$, we conclude that b_1 is a basis for B. ∎

Proof. We know that $[O_K : O] = c < \infty$, since O_K and O are both quadratic orders. c acts like a mcm, then $cO_K \subset O$. This implies that $\mathbb{Z} \oplus cO_K \subset O$. We must compute $[O_K : \mathbb{Z} \oplus cO_K]$. If we take a basis of O_K using 1.1.1, $O_K = [1, x]$ and $\mathbb{Z} \oplus x\mathbb{Z} = [1, cx]$, we can compute the rank and we observe that $[O_K : \mathbb{Z} \oplus cO_K] = c$. Thus applying the last lemma we obtain that $O = \mathbb{Z} \oplus FO_K$.
Taking $x \geq 1$, $O = \mathbb{Z} \oplus cO_K$ is an order. O_K contains a $\mathbb{Q}-$basis of K; $\{\alpha_1, ..., \alpha_n\}$. By the definition of O, O contains the $\mathbb{Q}-$basis $\{c\alpha_1, ..., c\alpha_n\}$. Using the first part of the proof we obtain that $[O_K : O] = c$. ∎

Proposition 1.1.7. *The discriminant of an order O with conductor F is $F^2 d_K$.*

Proof. If we have a basis $\{1, x\}$ of O_K, we can obtain a basis of O, $\{1, Fx\}$. Using the properties of the discriminant, we have that

$$disc(1, Fx) = F^2 disc(1, x) = F^2 disc(K)$$

∎

Observation 1.1.8. *We can study when a field K has an order of discriminant d. We solve this problem looking for a solution to the equation $d_K f^2 = d$. In the other direction, we can know which rings of integers has orders of a given discriminant.*

1.2 Quaternion algebras

Definition 1.2.1. An algebra B over K is a *quaternion algebra* B if there exists a basis $\{1, i, j, ij\}$ for B as a $F-$vector space such that

$$i^2 = a,\ j^2 = b,\ ij = -ij\ \ for\ a, b \in F^\times$$

Observation 1.2.2. *Along the dissertation, we will use quaternion algebras over $\mathbb{Q}$. We can see our quaternion algebras as:*

$$\mathbb{Q} \oplus i\mathbb{Q} \oplus j\mathbb{Q} \oplus ij\mathbb{Q}$$

Definition 1.2.3. An *involution* is a $K-$linear map $^{-}: B \to B$ which satisfies:

1. $\overline{1} = 1$
2. $\overline{\overline{c}} = c \ \forall c \in B$
3. $\overline{cd} = \overline{d}\overline{c} \ \forall c, d \in B$

Also, we say that an involution is *standard* if $c\overline{c} \in K$.

Observation 1.2.4. *If we have an algebra $(a, b|K)$ over a field with $char(K) \neq 2$, then the map*

$$t + xi + yj + zk \to t - (xi + yj + zk)$$

is a standard involution, and it is unique.

Lemma 1.2.5. *A quadratic $K-$ algebra C (an algebra such that $dim_K C = 2$) is conmutative and has an unique standard involution.*

Proof. $C \cong K \oplus \alpha K$ for all $\alpha \in C$, then it is conmutative.
If $^{-} : C \to C$ is any standard involution, we have that for all $\alpha \in C$, $\alpha^2 - (\alpha + \overline{\alpha})\alpha + \alpha\overline{\alpha} = 0$. We can deduce that every involution must has this form $i : \alpha \to (\alpha + \overline{\alpha}) - \alpha$. This map extends to an unique involution because $(\alpha + \overline{\alpha}) - \alpha$ is also a root of the minimal polynomial. ∎

Corollary 1.2.6. *If a quaternion algebra B has a standard involution, then it is unique.*

Proof. If we choose a $\alpha \in B \setminus K$, we have that $K[\alpha]$ has a unique standard involution by 1.2.5. As the restriction is unique for all α, the involution is unique. ∎

Definition 1.2.7. The *reduced trace* (trd) and the *reduced norm* (nrd) are maps $B \to K$ defined as:

$$trd: \ \alpha \to \alpha + \overline{\alpha} \quad nrd: \ \alpha \to \alpha\overline{\alpha}$$

Theorem 1.2.8 (Wedderburn's Structure Theorem)**.** *Let A be a finite dimensional simple algebra over F. Then A is isomorphic to $M_n(D)$ where $D \cong End_A(N)$ is a division algebra over F with N a nonzero minimal right ideal of A.*

We can find its proof in [1, thm. 7.1.1] and uses deep theory of quaternion algebras.

Corollary 1.2.9. *If B is a quaternion algebra over K, either B is a division algebra, or $H \cong M_2(F)$.*

Proof. Using Wedderburn's Structure Theorem. ∎

Definition 1.2.10. A quaternion algebra B over K is *split* if $B \cong M_2(F)$

Definition 1.2.11. We say that a prime number p (or ∞) is *ramified* if $B_p = B \otimes_K K_p$ (or $B_p = B \otimes_K K_\infty$) is a division ring. Otherwise we say that B *splits*.

Proposition 1.2.12. *Let B and B' quaternion algebras over K. They are isomorphic if and only if $ram(B) = ram(B')$.*

Its proof is in [1, prop. 4.3.1] which is based on theory about quaternion algebras.
Let B be a quaternion algebra over F such that $F = Frac(R)$

Definition 1.2.13. A *lattice* M is a finite generated $R-$submodule with $MF = V$

Definition 1.2.14. An $R-$*order* $O \subseteq B$ is a $R-$lattice that is also a subring of B

From now on we are going to work with a quaternion algebra B over $\mathbb{Q}$ which is ramified at a prime N and ∞. Since the algebra ramifies at ∞, the elements a, b such that $i^2 = a$, $j^2 = b$ are less than zero $(a, b < 0)$.

Definition 1.2.15. Let R be an order in B. We say that I is a *left ideal* of R, if it is a lattice in B and it is stable under left multiplication by R.
We define the *right order* (or *left order*) of an ideal as $O_R(I) = \{b \in B : \ Ib \subset I\}$ (respectively $O_L(I) = \{b \in B : \ bI \subset I\}$)

Definition 1.2.16. The *inverse ideal* of I is defined as $I^{-1} = \frac{1}{n(I)}\overline{I}$, where $n(I) = mcd\{n(b) : b \in I\}$ and $\overline{I} = \{\bar{b} : \ b \in I\}$.

Observation 1.2.17.
1. *The right order of an $R-$ideal I, such that R is a maximal order is also a maximal order.*
2. *I^{-1} is a right ideal for R. Its left order is the right order of I.*

Definition 1.2.18. Let S be a quadratic order, let O be a quaternion order. We say that an $R-$algebra embedding $\phi : \ S \hookrightarrow O$ is *optimal* if

$$\phi(K) \cap O = \phi(S)$$

Observation 1.2.19. *If an embedding $\phi : \ S \hookrightarrow O$ is not optimal, then there exists a larger order $S \subseteq S'$ such that its embedding is optimal.*

1.3 Geometric background

Definition 1.3.1. A real *Lie group* is a $C^\infty-$real manifold G with an associated group structure

$$\cdot : \ G \times G \to G \quad inverse : \ G \to G$$

with $\cdot$ and $inverse$ $C^\infty-$morphisms. We denote by G_0 the connected component of $e \in G$.

Observation 1.3.2. *We can define a complex Lie group using complex analyitical manifolds and holomorphic maps instead of the smooth concepts.*

Since every Lie group is a manifold, a meaningfull question is "*what is its tangent space?*". The answer to this question coincides with the definition of *Lie algebra*. This concept is used in a lot of areas of mathematics. Later, when we will define the concept of an algebraic variety we will see that it is closely related to the topic of the dissertation.

Definition 1.3.3. Let k be a field of characteristic $\neq 2$. A *Lie algebra* $\mathfrak{g}$ over k is a $k-$vector space equipped with a bracket operation

$$[\cdot, \cdot] : \ \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

such that $[X, Y] = -[Y, X]$ and $[X, [Y, X]] + [Z, [X, Y]]] + [Y, [Z, X]] = 0$ for all $X, Y, Z \in g$.
We also define a *Lie subalgebra* $\mathfrak{h}$ of $\mathfrak{g}$ as a vector subespace such that $[\mathfrak{h}, \mathfrak{h}] \subseteq \mathfrak{h}$.

In order to obtain the tangent space of a Lie group, we fix e, the identity element of G, and we set the map

$$\begin{aligned} [\cdot, \cdot] : \ \mathfrak{g} \times \mathfrak{g} &\to \mathfrak{g} \\ (X, Y) &\to (UV - VU)_e \end{aligned}$$

with U, V the unique left $G-$invariant vector fields on G such that $U_e = X$ and $V_e = Y$. The space $T_e(G)$ (also named as $Lie(G)$) endowed with the map $[\cdot, \cdot]$ is a Lie algebra. In fact, there is a strong correspondence between Lie groups and Lie algebras.

Proposition 1.3.4. *Let G a real Lie group and $\mathfrak{g} = Lie(G)$ its Lie algebra. There is a one-to-one correspondence*

$$\{H \subseteq G \textit{ connected Lie subgroup}\} \longleftrightarrow \{\mathfrak{h} \subseteq \mathfrak{g} \textit{ Lie subalgebra}\}$$

We can find the proof of this theorem at [33, Ch.1 sec. 2]. Its proof uses deep theory about Lie groups and Lie algebras.

Definition 1.3.5. 1. We define the *inner conjugation* as the following map

$$\begin{aligned} G &\to Aut(G) \\ g &\to c_g(h) = ghg^{-1} \end{aligned}$$

2. The *adjoint representation of G* is defined as

$$\begin{aligned} Ad:\ G &\to GL(\mathfrak{g}) \\ g &\to d_e(c_g) \end{aligned}$$

where $d_e(\cdot)$ is the differential of the map.

3. The *adjoint representation of* $\mathfrak{g}$ is defined as

$$\begin{aligned} ad:\ \mathfrak{g} &\to End(\mathfrak{g}) \\ a &\to d_e(Ad) \end{aligned}$$

Observation 1.3.6. *Using those maps, we can see the connection between a Lie algebra and its automorphisms set. Let $\mathfrak{g}$ be a real algebra. We can see $GL(\mathfrak{g})$ as a Lie group. By definition, this implies that its tangent space is a Lie algebra. $Lie(GL(\mathfrak{g})) = End(\mathfrak{g})$ since $GL(\mathfrak{g})$ is a linear space. Also, by the definition of the previous map, the adjoint representation of $\mathfrak{g}$ is a subalgebra of $End(\mathfrak{g})$. Using the previous proposition, we can deduce that there exists a connected Lie subgroup $Int(\mathfrak{g}) \subseteq GL(\mathfrak{g})$ such that $Lie(Int(\mathfrak{g})) = ad(\mathfrak{g})$.*

Definition 1.3.7. We say that a real Lie algebra is *compact* if $Int(\mathfrak{g})$ is compact.
A Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is *compactly embedded* in $\mathfrak{g}$ if $Int_g(\mathfrak{h}) \subset GL(\mathfrak{g})$ such that $Lie(H) = ad_g(\mathfrak{h})$ is compact.

Definition 1.3.8. A Lie algebra $\mathfrak{g}$ is *simple* if it is not abelian and it contains no ideals different from the trivial ones.
It is *semisimple* if it contains no abelian ideals such that $\mathfrak{a} \neq 0$.

We define the Killing form on $\mathfrak{g}$, which allows us to classify our Lie algebras. It is defined as follows

$$\begin{aligned} B_g:\ \mathfrak{g} \times \mathfrak{g} &\to k \\ (X, Y) &\to Tr(ad(X) \cdot ad(Y)) \end{aligned}$$

Theorem 1.3.9 (Cartan)**.** *Let k be a subfield of $\mathbb{C}$:*

1. *$\mathfrak{g}$ is semisimple if and only if $B_{\mathfrak{g}}$ is nondegenerate.*

2. *$\mathfrak{g}$ is semisimple if and only if $\mathfrak{g} \simeq \mathfrak{g}_1 \oplus ... \oplus \mathfrak{g}_r$ with $\mathfrak{g}_i$ simple Lie algebras.*

Also, if our Lie algebra $\mathfrak{g}$ is semisimple, given an ideal $\mathfrak{a} \subset \mathfrak{g}$, we can divide the algebra as $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^{\perp}$ with $\mathfrak{a}^{\perp} = \{X \in \mathfrak{g} :\ B_{\mathfrak{g}}(X, \mathfrak{a}) = 0\}$. We will name this type of decomposition by *reductive decomposition.*

Definition 1.3.10. We say that a Lie algebra is *reductive* if for any ideal $\mathfrak{a} \subset \mathfrak{g}$ there exists an ideal $\mathfrak{b} \subset \mathfrak{g}$ such that $\mathfrak{g} \simeq \mathfrak{a} \oplus \mathfrak{b}$.

Theorem 1.3.11. *A Lie algebra $\mathfrak{g}$ is reductive if and only if $\mathfrak{g} \simeq \mathfrak{s} \oplus \mathfrak{z}$ with $\mathfrak{s}$ a semisimple Lie algebra and $\mathfrak{z}$ an abelian Lie algebra.*

Classification of Lie groups:

1. We say that a Lie group G is a *torus* if it can be embedded as a subgroup of $\{diag(a_1, ..., a_n)\} \subset GL_n(\mathbb{C})$. We can see the space of diagonal matrices as $D_n \simeq \mathbb{C}^* \times ... \times \mathbb{C}^*$.

2. We say that a Lie group is *simple* if it is not abelian and it does not contain normal connected Lie subgroups that are not the trivial ones.

3. A Lie group is *semisimple* if it does not contain normal connected abelian Lie subgroups $\neq \{1\}$.

4. A Lie group is called *reductive* if the only normal connected abelian Lie subgroups are tori.

Even thought the theory about Lie groups and Lie algebras is beautifull per se, we are going to use those objects because they are closely related to the geometry. We are going to study certain manifolds such that their automorphism group is a Lie group. In that point we will be able to obtain properties of the manifold using the theory about Lie groups.
In a similar way as in Riemannian geometry we can define a metric over a complex analytic manifold M

$$\rho : \ T(M) \otimes T(M) \to \mathbb{C}$$

If ρ is $\mathbb{C}-$linear on the first variable, $\rho_p(u, v) = \overline{\rho_p(v, u)}$ $\forall u, v \in T_p(M)$ and $\rho(u, u) > 0$ $\forall u \in T_p(M) \setminus \{0\}$, we say that ρ is a *hermitian metric*. We will say that (M, ρ) is a *hermitian complex manifold*.

Definition 1.3.12. A *hermitian symmetric manifold* is a connected hermitian manifold (M, ρ) such that

1. M is *homogeneous*: the group $Aut(M, \rho)$ of holomorphic isometries acts transitively on M.

2. M is *symmetric*: $\forall p \in M$ there exists a map $s_p \in Aut(M, \rho)$ such that $s_p^2 = 1$, with the property that p is an isolated fixed point.

Observation 1.3.13. *A way to visualize how is the map s_p studying its action via local geodesics. Let M be a manifold (it can be a riemannian manifold, the definition is analogous). If we fix a point $p \in M$, we can obtain the local geodesics of p, parameterizing them so that $\gamma(0) = p$ with γ local geodesic of p. γ acts as follows: $s_p(\gamma(t)) = \gamma(-t)$.*

Example 1.3.14. *A complex elliptic curve with the metric $\rho = dxdy$ is a hermitian symmetric manifold. $E = \mathbb{C}/\Lambda$, with Λ a lattice over $\mathbb{C}$. The group E acts transitively by translations on M. If we fix a point $p \in E$, we can find the map $s_p : \ q \to 2p - q$, that is a symmetry which fixes p.*

Definition 1.3.15. Let (M, ρ) be a hermitian symmetric manifold, let $K_p(E)$ be the Gauss sectional curvature respect p and $E \subseteq T_p(M)$ such that $dim(E) = 2$.

1. If $K_p(E) < 0$, we say that (M, ρ) is of *noncompact type* also called *hermitian symmetric domain.*

2. If $K_p(E) > 0$, we say that (M, ρ) is of *compact type.*

3. If $K_p(E) = 0$ we say that (M, ρ) is of *euclidean type.*

When (M, ρ) is a hermitian symmetric manifold, we can define a topology over $G = Aut(M, \rho)$, with a basis of open subsets as follows

$$W(C, U) = \{g \in G : \ g(C) \subset U\} \tag{1.1}$$

where $C \subset M$ is compact and $U \subset M$ is open. With this topology, G admits an unique structure of real analytic Lie group.

There exists a canonical hermitian metric, the *Bergam's metric* g_{Bgm}. Let $D \subset \mathbb{C}^n$ be a bounded open subset. If the group $Hol(D)$ acts transitively and each point admits a symmetry, (D, g_{Bgm}) is an hermitian symmetric domain. Conversely, if we have an hermitian symmetric domain, it is isometric to some (D, g_{Bgm}) with $D \subset \mathbb{C}^n$ open and compact.
If we fix a point $p \in M$, we can define the following automorphism

$$\begin{aligned} \sigma \ : G &\to G \\ g &\to s_p g s_p \end{aligned}$$

this is clearly an involution on G. We can divide $\mathfrak{g} = Lie(G)$ as $\mathfrak{g} = \mathfrak{g}^+ \oplus \mathfrak{g}^-$ with $\mathfrak{g}^+$, $\mathfrak{g}^-$ the $\pm 1-$eigenspaces with respect to $d_e(\sigma)$.

Theorem 1.3.16. *Let (M, ρ) be an hermitian symmetric domain and let $K = K_p$ the isotropy group of p.*

1. *M is simply connected and G is semisimple and noncompact.*

2. *$Z(G) = \{g \in G : \ gh = hg \text{ for all } h \in G\} \subset K$ is a finite group. There exists a diffeomorphism*

$$\begin{aligned} \pi : \ G_0/K &\to M \\ g &\to g(p) \end{aligned}$$

3. *$(K_\sigma)_0 \subseteq K \subseteq K_\sigma = \{g \in G : \ \sigma(g) = g\}$ and $Lie(K) = \mathfrak{g}^+$.*

4. *There are two isomorphisms; $d_e\pi : \ \mathfrak{g}^- \to T_p(M)$ and $exp : \ K \times \mathfrak{g}^- \to G_0$.*

Definition 1.3.17. A Lie algebra $\mathfrak{g}$ is *compact* if $\mathfrak{g} = Lie(G)$ with G compact Lie group.

Definition 1.3.18. Let $\mathfrak{g}$ be a semisimple real algebra. We say that $s \in End(\mathfrak{g})$ is a *Cartan involution* if $s \neq Id$, $s^2 = Id$, and the $+1-$eigenspace of s, $\mathfrak{g}^+$ is compactly embedded in $\mathfrak{g}$.

Definition 1.3.19. We say that $(\mathfrak{g}, s)$ is a *symmetric Lie algebra.* Also we say that it is of compact type or noncompact type depending wether $\mathfrak{g}$ is compact or not.
We also say that $(\mathfrak{g}, s)$ is *irreducible hermitian noncompact symmetric Lie algebra* if satisfies that:

1. $\mathfrak{g}$ is noncompact, $\mathfrak{g}$ and $\mathfrak{g} \otimes \mathbb{C}$ are simple.

2. $\mathfrak{g}^+$ is a maximal proper subalgebra of $\mathfrak{g}$ and $z(\mathfrak{g}^+) \neq \{0\}$.

Theorem 1.3.20. *There exist a one-to-one correspondence between*

$$\left\{\begin{matrix} \textit{Irreducible hermitian} \\ \textit{symmetric domains.} \end{matrix}\right\} \to \left\{\begin{matrix} \textit{Irreducible noncompact hermitian} \\ \textit{symmetric Lie algebras.} \end{matrix}\right\}$$

Proof. If we have (M, ρ) an irreducible symmetric domain, we have that $d_e\sigma$ is a Cartan involution. Using 1.3.16, $\mathfrak{g}^+ = Lie(K)$. We know that K is compact, then $\mathfrak{g}^+$ is compact. We apply the same reasoning to deduce that $\mathfrak{g}$ is noncompact. We conclude saying that $(\mathfrak{g}, d_e\sigma)$ is an irreducible noncompact hermitian symmetric domain.
Conversely, let $(\mathfrak{g}, s)$ be an irreducible noncompact hermitian symmetric Lie algebra. Lets denote by $\widetilde{G}$ the universal covering of $Int(\mathfrak{g})$. $Lie(\widetilde{G}) = \mathfrak{g}$, and $\widetilde{G}$ is simply connected. We can find an involution $\sigma \in Aut(\widetilde{G})$ such that $d_e\sigma = s$.
We denote by $\widetilde{K}$ the connected component of e in $K_\sigma = \{g \in \widetilde{G} : \ \sigma(g) = g\}$. Using 1.3.16, $Lie(\widetilde{K}) = \mathfrak{g}^+$, and $\widetilde{K}$ is a maximal connected proper Lie subgroup of $\widetilde{G}$.

We define $M = \widetilde{G}/\widetilde{K}$, this is naturally a real analytic manifold. The base point is the image of $e \in \widetilde{G}$ by the map $\pi : \widetilde{G} \to M$. We define the action of $\widetilde{G}$ by multiplication. This action is transitive. There exists a lemma such that gives us the existence of a symmetry for M. With this lemma we conclude that (M, ρ) is an irreducible hermitian symmetric domain, with ρ the Riemannian metric, such that $\widetilde{G}$ acts on M by isometries. ∎

As we said in the introduction, Shimura varieties are a generalization of modular curves. We can express every modular curve as a quotient

$$\mathcal{H}/\Gamma$$

Defining hermitian symmetric domains, we have generalized the complex half plane. We still need to find the generalization for congruence subgroups. As we saw, we have an action of $Aut(M, \rho)$ on M, then, we have to find certain subgroups such that the quotients makes sense. Those subgroups are given by the following proposition

Proposition 1.3.21. *Let D be a hermitian symmetric domain, then let $G = Aut(D)$ be the group of holomorphic isometries of D. Let $\Gamma \subset G^+$ be a discrete torsion-free subgroup. Thus there is an unique complex analytic structure on $D(\Gamma) = D/\Gamma$ such that*

$$\pi : D \to D(\Gamma)$$

is a local isomorphism. Also, we say that a map of complex analytic varieties $D(\Gamma) \to V$ is analytic if the following composition

$$D \to D(\Gamma) \to V$$

is an analytic map.

Proof. As with modular curves. If we endow the quotient with the quotient topology, $D(\Gamma)$ is a separeted space. Then we take $p \in D$ and its isotropy group $\Gamma_p \subset K_p$. Since Γ is a discrete subgroup, then Γ_p is a discrete subgroup of a compact group, and then finite. Using the hypothesis of being torsion free, we have that $\Gamma_p = \{1\}$ for all $p \in D$. Then there exist a point $p \in U_p$ such that

$$\gamma U_p \cap U_p = \varnothing$$

for all $\gamma \in \Gamma \setminus \{1\}$. Thus the restricted map

$$\pi|_{U_p} : U_p \to \pi(U_p)$$

is an homeomorphism, giving us a complex analytic atlas for $D(\Gamma)$. ∎

The holomorphic isometries group is a Lie group. Since the structure of that Lie groups can be very complicated, we need to change to an easier object. We are going to simplify this problem introducing a new concept, algebraic groups. With an algebraic group G we always have an embedding

$$G \hookrightarrow GL(\Omega)$$

that will allows us to see elements of the algebraic group as matrices, which allows us to reduce our problems to linear problems.

Definition 1.3.22. An *algebraic group* is an algebraic variety G with morphisms

$$G \times G \to G \text{ such that } (x, y) \to xy$$
$$inverse : G \to G \text{ such that } x \to x^{-1}$$

satisfying the usual group axioms.

We are going to work only with *affine algebraic groups*. We can see this varieties as Zariski-closed subgroups of $GL_n(\Omega)$ with Ω algebraically closed field having infinite trascendence degree over their prime subfield.

Definition 1.3.23. Let G be an algebraic group over k. We define the *derived group*, G^{der} as the intersection of the normal algebraic groups of G such that G/N is conmutative.
We define G^{ad} as the quotient $G/Z(G)$. Also, we define $G(\mathbb{R})_+$ as the group of elements whose image in $G^{ad}(\mathbb{Q})$ lies in the identity component $G(\mathbb{R})^+$. Then, $G(\mathbb{Q})_+ = G(\mathbb{Q}) \cap G(\mathbb{R})^+$.

Examples 1.3.24 (Important algebraic groups)**.**

1. *$\mathbb{G}_m = Spec\ k[X,Y]/(XY-1)$ is the multiplicative group. Its main propery is that for any $k-$algebra A, we have that $\mathbb{G}_m(A) = A^*$.*
2. *$\mathbb{G}_a = Spec\ k[X]$, is the additive group, we have that $G_a(A) = A$ for any $k-$algebra A.*
3. *M_n, GL_n, SO_n, SP_{2n},...*

Definition 1.3.25. We can classify connected algebraic groups G over k as follows

1. G is a *torus* if $G \otimes \overline{k} \simeq \mathbb{G}_m \times \overset{n}{\cdots} \times \mathbb{G}_m$. We denote the minimal field extension K such that $G \otimes K = \mathbb{G}_m \times \overset{n}{\cdots} \times \mathbb{G}_m$ as the *splitting field* of G.
2. An algebraic group G is *semisimple* if it contains no smooth connected normal commutative algebraic subgroups different from the identity.
3. The algebraic group G is *reductive* if it contains no smooth connected normal commutative algebraic subgroups other than tori.

We construct a very important operator on algebraic groups, the reduction $Res_{K/F}$. The idea is that we have an algebraic group G defined over F and we have a galois finite field extension K/F, then we want to know how are the points of G over K. This is explained in section 4 of [13], starting as an example with GL_n. We are going to use this operator along the dissertation. This is beause the reduction of the multiplicative group $\mathbb{G}_m$ has good properties and is well defined. We set $T = Res_{K/F}\mathbb{G}_m$, then

$$T(A) = (A \otimes_F K)^*$$

Where $T(A)$ are the $A-$points for the algebraic group T. We can see its $A-$points as

$$G(A) = \{Spec\ (A) \to Spec(R) = G\} = Hom\{R \to A\}$$

We observe that the operator $Res_{K/F}$ creates a relation

$$\{\mathit{Varieties\ over}\ K\} \longleftrightarrow \{\mathit{Varieties\ over}\ F\}$$

Definition 1.3.26. Two subgroups $S_1, S_2 \subset S$ of a group S are *conmensurable* if $S_1 \cap S_2$ has finite index in S_1 and S_2.

Definition 1.3.27. Let G be an algebraic group over $\mathbb{Q}$. We say that a group $\Gamma \subset G(\mathbb{Q})$ is *arithmetic* if it is conmensurable with $G(\mathbb{Q}) \cap GL_n(\mathbb{Z})$ for some embedding $G \hookrightarrow GL_n$.
A congruence subgroup of $G(\mathbb{Q})$ is a subgroup Γ such that for some embedding as before, the group contains

$$\Gamma(N) = G(\mathbb{Q}) \cap \{g \in GL_n(\mathbb{Z})\ s.t\ g \equiv Id_n\ mod\ N\}$$

as a subgroup of finite index.

The holomorphic isometries group is a Lie group. Then we have to define the same notions over Lie groups.

Definition 1.3.28. Let G be an arbitrary connected real Lie group, we say that a group Γ is an *arithmetic subgroup* if

- There exists an algebraic group $\mathfrak{G}$ over $\mathbb{Q}$.
- There exists an arithmetic subgroup $\hat{\Gamma} \subset \mathfrak{G}(\mathbb{Q})$.
- There exists a surjective morphism $\pi : \mathfrak{G}(\mathbb{R})^+ \to G$ with compact kernel such that $\pi(\hat{\Gamma}) = \Gamma$.

The aim of this section is to prove the Baily-Borel's theorem. This is a very important theorem in algebraic geometry, which gives a criterion to determine when a quotient is an algebraic manifold. From now on, we are going to denote by $\Gamma \subset G_0$ to an arithmetic torsion free-subgroup.

Theorem 1.3.29 (Baily-Borel)**.** *1. If we have D and Γ as before, we have that $D(\Gamma)$ has a canonical realization as a smooth Zariski-open subset of a projective algebraic variety $D(\Gamma)^*$. By the arithmetic subgroup, we have an algebraic group with a surjective homomorphism*

$$\pi : \mathfrak{G}(\mathbb{R})^+ \to G$$

then, the theorem states that if $\mathfrak{G}(\mathbb{Q})$ contains no unipotent elements, then $D(\Gamma)$ is compact

2. Let V be a non-singular quasi-projective variety over $\mathbb{C}$. Every holomorphic map of complex analytic manifolds

$$f : V(\mathbb{C}) \to D(\Gamma)(\mathbb{C})$$

is a regular algebraic map.

To prove this theorem, we will need two theorems.

Theorem 1.3.30 (Chow)**.** *Every closed analytic subset of $\mathbb{P}^n$ is an algebraic set. Also if*

$$f : X \to Y$$

is holomorphic, then f is a regular map.

To apply Chow's theorem to our proof, we have an important tool, called *the canonical embedding*. When we have a complex analytic variety $D(\Gamma)$, we have defined its differentials, $\Omega^1(D(\Gamma))$. We define the following map

$$\begin{aligned} D(\Gamma) &\hookrightarrow \mathbb{P}^{g-1} \\ [\tau] &\to [f_1(\tau) : \ldots : f_g(\tau)] \end{aligned}$$

with f_i functions such that $\Omega(D(\Gamma)) = \langle f_1 d\tau, \cdots, f_g d\tau \rangle$. These maps are modular forms of weight 2. This map usually is not an embedding, but if $g > 1$ and $D(\Gamma)$ is not hyperelliptic, we have that the previous map is an embedding.

Proof of Baily-Borel theorem for modular curves.

For modular curves we have that $D = \mathcal{H}$, $\rho = \frac{dxdy}{y^2}$, and $G = PSL_2(\mathbb{R})$. The algebraic group is $\mathfrak{G} = SL_2(\mathbb{Q})$, and the map between these two groups is

$$\mathfrak{G}(\mathbb{R}) \to G = \mathfrak{G}/\pm I$$

The action on $\mathcal{H}$ is given by linear transformations. The arithmetic subgroups of this group are congruence subgroups. We can see those groups thought the map as

$$\Gamma = \hat{\Gamma}/\pm I$$

with $\hat{\Gamma}$ congruence subgroup.
Also, we know that modular curves have a topological structure and a Riemann surface structure, we can see this construction in [22, p. 45] and [22, p. 48]. Also, we have the same structures defined on its compactification, [22, p. 58].
We need to prove that $D(\Gamma) \subseteq D(\Gamma)^*$ is a Zariski open set of a projective space. As modular forms form a basis of $\Omega(\mathcal{H}/\hat{\Gamma})$ we have an embedding of $D(\Gamma)^*$ on $\mathbb{P}^n$. Applying Chow's theorem, $D(\Gamma^*)$ is naturally a projective variety and $D(\Gamma) = D(\Gamma)^* \setminus (\Gamma \setminus \mathbb{P}^1(\mathbb{Q}))$. ∎
The whole proof of this theorem can be found at [9, p. 24]. It uses automorphic forms to obtain the embeddings and Big Picard Theorem to the second part.

Corollary 1.3.31. *1. The structure of an algebraic variety on $D(\Gamma)$ is unique.*

2. For any other compactification $D(\Gamma) \hookrightarrow D(\Gamma)^{*\ new}$ such that $D(\Gamma)^{*\ new}$ is a projective variety with $D(\Gamma)^{*\ new} \setminus D(\Gamma)$ a divisor with normal crossings, there exists a unique regular map $D(\Gamma)^{*\ new} \to D(\Gamma)^*$ such that the following diagram conmutes

$$\begin{array}{ccc} D(\Gamma) & \hookrightarrow & D(\Gamma)^{*\ new} \\ \downarrow & & \downarrow \\ D(\Gamma)^* & \xrightarrow{id} & D(\Gamma)^* \end{array}$$

Proof. 1. Using Borel's theorem we know that there exists an algebraic variety V such that

$$D(\Gamma) \simeq V(\mathbb{C})$$

Then, since this is an ismorphism, we have that the structure is unique.

2. Using Borel's theorem we have the following diagram

$$\begin{array}{ccc} V(\mathbb{C}) & \xrightarrow{f} & D(\Gamma) \\ \downarrow & & \downarrow \\ V^*(\mathbb{C}) & \xrightarrow{\hat{f}} & D(\Gamma)^* \end{array}$$

If f is holomorphic, then by Borel's theorem $\hat{f}$ is a regular map between algebraic varieties. Then, appliying this theorem to $V = D(\Gamma) \subset V^* = D(\Gamma)^{*\ new}$ the statement holds.

∎

This theorem will prove that Shimura varieties are in fact algebraic varieties. Since this theorem will be used along the dissertation, we will give some examples of aplications of Borel's theorem, which will appear along the second chapter.

Examples 1.3.32.

- *The basic examples are modular curves. We take $D = \mathcal{H}$, its holomorphic isometries are $Aut(\mathcal{H}) = SL_2(\mathbb{R})$, with $G = SL_2$ semisimple algebraic group over $\mathbb{Q}$. We take $\Gamma = SL_2(\mathbb{Z})$, and then we can embed this quotient in the affine space*

$$D(\Gamma) \xrightarrow{\simeq} \mathbb{A}^1_{\mathbb{C}}$$

We can observe that this is not a projective variety, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ is unipotent.

- *Let $D = \mathcal{H}_n$ the Siegel half plane, a generalization of the complex half plane using matrices. We can see its explicit definition in chapter 2 section 3. The group $G = Sp_{2n}$ acts on the Siegel half plane, also this group is defined over $\mathbb{Q}$ and it is semisimple. Then the quotient*

$$SP_{2n}(\mathbb{Z}) \setminus \mathcal{H}$$

is the set of complex points of a non-projetive variety.

- *This case will be very important along the dissertation. Let B be a quaternion algebra over a totally real field F. We denote by $v_1, ..., v_n : F \hookrightarrow \mathbb{R}$ each real archimedian place of B. Then we write $B \otimes_{\mathbb{Q}} \mathbb{R} = B \otimes_F F \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_v (B \otimes_f \mathbb{R}_v) = M_2(\mathbb{R}) \times \overset{r}{\cdots} \times M_2(\mathbb{R}) \times \mathbb{H} \times \overset{s}{\cdots} \times \mathbb{H}$ with $n = r + s$.*

  Let $B^* = \{b \in B^*\ s.t\ N(b) = 1\}$, this is an algebraic group over F, because in every representation of the quaternion algebra, the norm will be determined by the determinant of a matrix, providing us a polynomial equation which defines the algebraic group.
  Set $G_B = Res_{F/\mathbb{Q}} B^*$, that is also an algebraic group over $\mathbb{Q}$ by definition, it has the property that $G_B(K) = (B \otimes_{\mathbb{Q}} K)^*$ for any extension field $K/\mathbb{Q}$. Using the previous isomorphisms

given by archimedean places we have that $G_B(\mathbb{R}) = SL_2(\mathbb{R}) \times \overset{r}{\cdots} \times SL_2(\mathbb{R}) \times \mathbb{H}^* \times \overset{s}{\cdots} \times \mathbb{H}^*$.

Let $\mathcal{O}$ *be a quaternion order, we can define the quaternion order of norm* 1 *as* $\mathcal{O}$. *We claim that this is a discrete subgroup of* $G_B(\mathbb{R})$, *and it is in fact and arithmetic subgroup of*

$$G = SL_2(\mathbb{R}) \times \overset{r}{\cdots} \times SL_2(\mathbb{R})$$

This is because the kernel of

$$G_B(\mathbb{R}) \to G$$

is compact. We have that this group acts on

$$D = \mathcal{H}_1 \times \overset{r}{\cdots} \times \mathcal{H}_1$$

We use the Baily Borel's theorem, concluding that for any subgroup

$$\Gamma \subset G$$

which satisfies the hypothesis $D(\Gamma)$ *is a quasi-projective variety. We are going to examine specific cases of quaternion algebras*

- *Let* $B \simeq M_2(F)$. *In this quaternion algebra there are unipotent elements, then* $D(\Gamma)$ *is not compact*
- *If* $B = M_2(\mathbb{Q})$, *and* $\Gamma \in SL_2(\mathbb{Z})$ *is a subgroup as in the previous theorem, using Baily Borel we can define its quotinent, that is a modular curve.*
- *If* $F \neq \mathbb{Q}$ *and* $B = M_2(F)$, *then* $D(\Gamma)^*$ *are called Hilbert-Blumenthal modular variety. This is a singular projective variety of dimension* $[F : \mathbb{Q}]$.
- *If* $B \not\simeq M_2(F)$, *then there are no unipotent elements in any* Γ. *The variety is compact and* $D(\Gamma) = D(\Gamma)^*$ *is a projective variety of dimension* r. *We can claim that this variety is smooth unless* Γ *has torsion.*

All those examples are in fact Shimura varieties, specifically quaternionic Shimura varities. We will study those objects in the sections 5, 6 *and* 7 *of the second chapter.*

Chapter 2

Shimura varieties

2.1 Adeles

To ilustrate the behaviour of Shimura varieties the study of the ring of adeles is indispensable, this is because the arithmetic of Shimura varieties will be encoded in the "adele world". Before starting to define what are the adeles, we are going to give a brief overview of how arises this concept.

Let $\mathfrak{L}_n(\mathbb{Q})$ be the space of lattices in $\mathbb{Q}^n$. Let $L \in \mathfrak{L}_n(\mathbb{Q})$. For every prime p we can define its localization as

$$L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p \subset \mathbb{Q}_p^n$$

L_p is a lattice in $\mathbb{Q}_p^n$. Our main objective is to obtain information about the global lattices using the local reduction, which is simpler. To connect the global and the local information we have the following property which proof can be found at [13, p. 10].

Proposition 2.1.1. *Let $L \subset \mathbb{Q}^n$ be a lattice. For almost every prime p, then*

$$L_p = \mathbb{Z}_p^n$$

Moreover, the map

$$L \to (L_p) \text{ with } p \text{ prime.}$$

Defines a bijection between the set of lattices $\mathfrak{L}_n$ and the set of sequences L_p, with p prime such that $L_p = \mathbb{Z}_p^n$ for almost all p.
The converse map is defined as

$$(L_p)_p \to L = \bigcap_p (\mathbb{Q}^n \cap L_p)$$

This proposition essentially tells us that the set of global lattices is determined by a certain type of local lattices, and then we can obtain information about global lattices studying local lattices. The idea behind adéles is to keep all the local data in one structure.
Now, we can observe that the group $GL_n(\mathbb{Q}^n)$ acts transitively on $\mathfrak{L}_n(\mathbb{Q})$ by a linear change of variable

$$L \to Lg = \{g^{-1}x,\ x \in L\}$$

We deduce that the stabilizer of $\mathbb{Z}^n$ is $GL_n(\mathbb{Z})$. Then

$$\mathfrak{L}_n(\mathbb{Q}) = \mathbb{Z}^n GL_n(\mathbb{Q}) \simeq GL_n(\mathbb{Z}) \setminus GL_n(\mathbb{Q})$$

If we look at the local case, let $\mathfrak{L}_n(\mathbb{Q}_l)$ be the set of lattices in $\mathbb{Q}_p^n$. The group $GL_n(\mathbb{Q}_p)$ acts transitively on $\mathfrak{L}_n(\mathbb{Q}_p)$, and the stabilizer of $\mathbb{Z}_p^n$ is $GL_n(\mathbb{Z}_p)$. Then, with the same action, we can obtain that

$$\mathfrak{L}_n(\mathbb{Q}_p) = GL_n(\mathbb{Q}_p)\mathbb{Z}_p \simeq GL_n(\mathbb{Q}_p) \setminus GL_n(\mathbb{Z}_p)$$

This identification, together with the proposition, allows us to define the *restricted product*

$$\prod_p{}' \mathfrak{L}_n(\mathbb{Q}_p) = \{(L_p)_p \ s.t\ L_p \in \mathfrak{L}_n(\mathbb{Q}_p),\ L_p = \mathbb{Z}_p^n \ for\ almost\ all\ p\}$$

We can also deduce that $\mathfrak{L}_n(\mathbb{Q})$ is acted transitively by the *restricted product*

$$GL_n(\mathbb{A}_f) = \prod_p{}' GL_n(\mathbb{Q}_p) = \{(g_p)_p \ s.t\ g_p \in GL_n(\mathbb{Z}_p)\ for\ almost\ all\ p\}$$

From this action, we can obtain the equivalent global action. Given $g_f = (g_p)_p \in \prod_p' GL_n(\mathbb{Q}_p)$, then

$$g_f L = \bigcap_p (\mathbb{Q}^n \cap g_p L_p)$$

The group $GL(\mathbb{A}_f)$ is called *the group of finite adelic points of GL_n.*

Observation 2.1.2. *We have an embedding*

$$\begin{aligned} GL_n(\mathbb{Q}) &\hookrightarrow GL_n(\mathbb{A}_f) \\ \gamma &\to (\gamma, \gamma, ...)_p \end{aligned}$$

Now, we can express the set of lattices of $\mathbb{Q}^n$ with its new definition as

$$\mathfrak{L}_n(\mathbb{Q}) \simeq GL_n(\mathbb{Z}) \setminus GL_n(\mathbb{Q}) \simeq GL_n(\mathbb{A}_f)/GL_n(\widehat{\mathbb{Z}})$$

with $GL_n(\widehat{\mathbb{Z}}) = \prod_p GL_n(\mathbb{Z}_p)$. We can also give another expression of the set of lattices, which will be crucial in the dissertation.
Since $GL_n(\mathbb{Z}) = GL_n(\mathbb{Q}) \cap GL_n(\widehat{\mathbb{Z}})$, we define the map

$$\begin{aligned} GL_n(\mathbb{Q}) &\to GL_n(\mathbb{Q}) \times GL_n(\mathbb{A}_f) \\ g &\to (g, Id) \end{aligned}$$

This map induces the main identification

$$\mathfrak{L}_n(\mathbb{Q}) \simeq GL_n(\mathbb{Z}) \setminus GL_n(\mathbb{Q}) \simeq GL_n(\mathbb{Q}) \setminus GL_n(\mathbb{Q} \times GL_n(\mathbb{A}_f)/GL_n(\widehat{\mathbb{Z}})$$

In this expression, $GL_n(\mathbb{Q})$ acts diagonally by left multiplication on $GL_n(\mathbb{Q}) \times GL_n(\mathbb{A}_f)$. We also can define the equivalent double quotient for real lattices, and we denote by $GL_n(\mathbb{A}) = GL_n(\mathbb{R}) \times GL_n(\mathbb{A}_f)$, the *group of adelic points of GL_n.*

We have defined this concepts for GL_n, which is an algebraic group. Now we are going to define *adeles*, and *ideles*, with the objective of defining adelic points of any algebraic group.

Definition 2.1.3. The ring of *finite adeles* is the following restricted product

$$\mathbb{A}_f = \prod_p{}' \mathbb{Q}_p = \{(\lambda_p)_p \ s.t\ \lambda_p \in \mathbb{Q}_p,\ \lambda_p = \mathbb{Z}_p \ for\ a.e.p\}$$

The ring of *adeles* is the product

$$\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$$

Observation 2.1.4. *Since adeles are defined over locally compact rings as $\mathbb{R}$ and $\mathbb{Q}_p$, we can define its natural topology. A basis of open subsets is given by*

$$\Omega_\infty \times \prod_{p \in S} \Omega_p \times \prod_{p \notin S} \mathbb{Z}_p$$

where S is a finite subset of primes, $\Omega_v \subset \mathbb{Q}_v$ are open subsets in the v-adic topology and Ω_∞ is an open subset of $\mathbb{R}$. It is important to remark that, with this topology, the embeddings $\mathbb{Q}_p \hookrightarrow \mathbb{A}_f$, $\mathbb{R} \hookrightarrow \mathbb{A}$ and $\mathbb{A}_f \hookrightarrow \mathbb{A}$ are closed.

Let V be any algebraic variety defined over $\mathbb{Q}$, we can define its adelic points as in the way that we have been doing

$$V(\mathbb{A}) = \prod_v{}' V(\mathbb{Q}_v) = \{(x_v)_v \ s.t\ x_v \in V(\mathbb{Q}_v),\ x_p \in \mathbb{Z}_p^n \ for\ a.e.p\}$$

Now, we can generalize all properties that we gave for the algebraic group GL_n. We have the embeddings

$$\begin{aligned} G(\mathbb{Q}_p) &\hookrightarrow G(\mathbb{A}_f) \\ g_f &\to (Id_{\mathbb{R}}, g_f) \end{aligned}$$

And then, we have the next embedding

$$\begin{aligned} G(\mathbb{Q}) &\hookrightarrow G(\mathbb{A}_f) \\ g_{\mathbb{Q}} &\to (g_{\mathbb{Q}}, (g_{\mathbb{Q}})_p) \end{aligned}$$

We can obtain the "integrality notions" using that the group $G(\mathbb{Z}_p) = G(\mathbb{Q}_p) \cap GL_n(\mathbb{Z}_p)$ is an open compact subgroup of $G(\mathbb{Q}_p)$ and $G(\widehat{\mathbb{Z}}) = G(\mathbb{A}_f) \cap GL_n(\widehat{\mathbb{Z}})$ is an open compact subgroup of $G(\mathbb{A}_f)$.

Now, we are going to study the generalization of the double quotient that we mentioned before. The properties of this object and the *strong aproximation* theorem, will give important tools for the theory of Shimura varieties.

Theorem 2.1.5 (Borel)**.** *The double quotient*

$$G(\mathbb{Q}) \setminus G(\mathbb{A})/G(\mathbb{R})G(\widehat{\mathbb{Z}})$$

is finite. The same result holds if we change $G(\widehat{\mathbb{Z}})$ by any compact subgroup $K_f \subset G(\mathbb{A}_f)$.

The proof of this theorem can be found in [13, p. 399], and uses advanced theory about algebraic groups.

Observation 2.1.6. *Even thought we have not proved the previous theorem, we can use the inclusion $G(\mathbb{A}_f) \subset G(\mathbb{A})$ to obtain an useful identification*

$$G(\mathbb{Q}) \setminus G(\mathbb{A}_f)/K_f \simeq G(\mathbb{Q}) \setminus G(\mathbb{A})/G(\mathbb{R})K_f$$

This gives us a way to express adelic points of an algebraic group as follows

$$G(\mathbb{A}) = \cup_i G(\mathbb{Q}) g_i G(\mathbb{R}) K_f,\ g_i \in G(\mathbb{A})$$

Rewriting $g_i = (g_{\mathbb{R},i}, g_{f,i})$, we can define a group that is conmensurable with $G(\mathbb{Z})$ and discrete in $G(\mathbb{R})$

$$\Gamma_i = GL_n(\mathbb{Q}) \cap g_{f,i} K_f g_{f,i}^{-1}$$

Proposition 2.1.7. *With the previous notation, we have the following homeomorphism*

$$\cup_i \Gamma_i \setminus G(\mathbb{R}) \simeq G(\mathbb{Q}) \setminus G(\mathbb{A})/K_f$$

Proof. Let $g \in G(\mathbb{A})$, and $[g] = G(\mathbb{Q}) g K_f$ expressed as in the previous coset form. We consider the map

$$\begin{aligned} \cup_i \Gamma_i \setminus G(\mathbb{R}) &\to G(\mathbb{Q}) \setminus G(\mathbb{A})/K_f \\ (i, \Gamma_i g_{\mathbb{R}}) &\to [(g_{\mathbb{R}}, g_{f,i})] \end{aligned}$$

This map respects the quotient. Let $\gamma \in \Gamma_i$. If we replace $g_{\mathbb{R}}$ by $\gamma_i g_{\mathbb{R}}$, we have that

$$[(\gamma g_{\mathbb{R}}, g_{f,i})] = [(g_{\mathbb{R}}, \gamma^{-1} g_{f,i})] = \tag{2.1}$$

where we have used the fact that if we multiply $g_{\mathbb{R}}$ by γ_i, it changea the $g_{f,i}$ part by the definition of the map. Also, we can use the fact that $\gamma_i \in GL_n(\mathbb{Q}) \cap g_{f,i} K_f g_{f,i}^{-1}$, and then we can express $\gamma_i = g_{f,i} k_f g_{f,i}^{-1}$

$$(2.1) = [(g_{\mathbb{R}}, g_{f,i} k_f g_{f,i}^{-1} g_{f,i})] = [(g_{\mathbb{R}}, g_{f,i})]$$

In the last equality we have used the fact that $k_f \in K_f$. Then, this step follows by quotient's definition.
This map is continuous and closed. We have to prove that it is also bijective. Lets suppose that $[(g_{\mathbb{R}}, g_{f,i})] = [(g'_{\mathbb{R}}, g_{f,i'})]$. Using where is this map defined, we have that

$$(g'_{\mathbb{R}}, g_{f,i'}) = (\gamma g_{\mathbb{R}}, \gamma g_{f,i} k_f)$$

Thus we conclude with $i = i'$ which implies that $g_{f,i} = gf, i'$ and $\gamma \in \Gamma_i$, deducing the injectivity. In order to prove the surjectivity let $g \in G(\mathbb{A})$ with $g = g_{\mathbb{R}} g_f$, by definition there exists i, $\gamma \in G(\mathbb{Q})$ and $k_f \in K_f$ such that $g_f = \gamma g_{f,i} k_f$. Then we can express $[g]$ as

$$[g] = [g_{\mathbb{R}}, \gamma g_{f,i} k_f] = [\gamma^{-1} g_{\mathbb{R}}, g_{f,i}]$$

∎

Theorem 2.1.8 (Strong aproximation)**.** *Let G be a semisimple, simply connected, algebraic group such that for each simple factor of G, its group of real points is not compact, then $G(\mathbb{Q})G(\mathbb{R})$ is dense in $G(\mathbb{A})$. In particular, for any open compact subgroup $K_f < G(\mathbb{A}_f)$, we have*

$$G(\mathbb{A}) = G(\mathbb{Q})G(\mathbb{R})K_f \text{ and } \Gamma \setminus G(\mathbb{R}) \simeq G(\mathbb{Q}) \setminus G(\mathbb{A})/K_f$$

$$\textit{Also } G(\mathbb{A}_f) = G(\mathbb{Q})K \textit{ with } K \textit{ compact open subgroup of } G(\mathbb{A}_f)$$

Proposition 2.1.9 (Real aproximation)**.** *Let G be a connected algebraic group over $\mathbb{Q}$. Then $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$*

We can find the proof of this proposition at "On sa ramène aisèment au cas des tores", written by Deligne or in [13, p. 399]. Its proof uses theory about algebraic groups and adeles.

2.2 Shimura varieties

Definition 2.2.1. A *connected Shimura datum* is a pair $(G, D = \{h\})$, where

- G is a semisimple algebraic group over $\mathbb{Q}$.
- $h: S^1 \to G^{ad}_{\mathbb{R}}$ is an homomorphism such that
  - *SV1:* Only the characters 1, z and $z^{-1} = \overline{z}$ occur in the adjoint representation of S^1 on $V = Lie(G^{ad})_{\mathbb{C}}$.
  - *SV2:* $Ad(h(-1))$ is a Cartan involution on $Lie(G^{ad})_{\mathbb{R}}$.
  - *SV3:* There exists no factor H of G^{ad} over $\mathbb{Q}$ such that $H(\mathbb{R})$ is compact.
- $D = \{g \cdot h \cdot g^{-1}\}_{g \in G^{ad}(\mathbb{R})_0} \subset Hom(S^1, G^{ad}_{\mathbb{R}})$.

Observation 2.2.2. *We denote by $G_A(R) = G(R) \otimes_R A$ for any field A and any R $A-$algebra.*

Observation 2.2.3. *We can explain the meaning of SV1 as follows; using the definition of the map Ad we have the following chain of maps*

$$S^1 \xrightarrow{h} G^{ad}_{\mathbb{R}} \xrightarrow{Ad} GL(Lie(G^{ad}_{\mathbb{R}}))$$

The composition map is a representation of S^1. This means that for each $z \in S^1$, we have associated a linear transformation of $Lie(G^{ad}_{\mathbb{R}})$. The hypothesis SV1 says that we can subdivide V as $V = V^0 \oplus V^+ \oplus V^-$ using the action of the linear transformations inherited from S^1 as follows:
$\forall z \in S^1$, we have that $Ad\ h(z)v_0 = v_0$, $Ad\ h(z)v_+ = zv_+$, $Ad\ h(z)v_- = z^{-1}v_-$, for any $v_0 \in V^0$, $v_+ \in V^+$ and $v_- \in V^-$.

Observation 2.2.4. *Condition SV3 will be usefull when G is simply connected to apply the Strong approximation theorem,2.1.8. This theorem will allow us to obtain information about the arithmetic properties of Shimura varieties.*

Lemma 2.2.5. *Let H be an adjoint real Lie group, and let $h : S^1 \to H$ be an homomorphism satisfying $SV1$, $SV2$. Then the following conditions on h are equivalent*

1. *$h(-1) = 1$.*
2. *h is trivial.*
3. *H is compact.*

Proof. $(1 \Rightarrow 2)$ If $h(-1) = 1$, we deduce that h can factor through

$$S^1 \xrightarrow{2} S^1$$

because h is an homomorphism. Then we observe that $z^{\pm 1}$ cannot occur in the representation of S^1 on $Lie(H)_{\mathbb{C}}$. Then S^1 acts trivially on $Lie(H)_{\mathbb{C}}$, implying 2.
$(2 \Rightarrow 1)$ trivial.
$(a \iff c)$. From [6, prop 1.17 a] we can use that given a connected algebraic group G over $\mathbb{R}$, $G(\mathbb{R})$ is compact if and only if the Cartan involution is the identity map.

$$H \text{ is compact} \iff ad\ h(-1) = id_G \iff h(-1) = 1$$

The last equivalence follows because $Z(H) = 1$. ∎

Proposition 2.2.6. *To give a connected Shimura datum is the same as to give*

1. *A semisimple algebraic group G over $\mathbb{Q}$ of noncompact type.*
2. *A hermitian symmetric domain D.*
3. *An action of $G(\mathbb{R})^+$ on D defined by a surjective homomorphism $G^{ad}(\mathbb{R})^+ \to Hol(D)^+$ with compact kernel.*

Proof. Let (G, D) be a connected Shimura datum. Let $h \in D$ that is of the following form

$$h : S^1 \to G$$

We can decompose $G^{ad}_{\mathbb{R}}$ into a product of its simple factors, obtaining

$$G^{ad}_{\mathbb{R}} = H_1 \times \cdots \times H_s$$

We can project the map h into the simple components of $G^{ad}_{\mathbb{R}}$. Let $u_i : S^1 \to G^{ad}_{\mathbb{R}} \xrightarrow{p_i} H_i$, where p_i is the projection to the $i-$th component. Since this map satisfies the hypothesis of the previous lemma, 2.2.5, we can deduce that $u_i = 1$ if H_i is compact. Otherwise, using [6, prop. 1.21], we deduce that there is an irreducible hermitian symmetric domain D'_i such that $H_i(\mathbb{R})^+ = Hol(D'_i)^+$,

and D'_i is in natural one-to-one correspondence with the set D_i of $H_i(\mathbb{R})^+-$conjugates of u_i.
The product $D' = \prod_i D'_i$ is a hermitian symmetric domain on which $G(\mathbb{R})^+$ acts via a surjective homomorphism $G^{ad}(\mathbb{R})^+ \to Hol(D)^+$ with compact kernel. Also, there is a natural identification

$$D' = \prod D'_i \longleftrightarrow D = \prod D_i$$

Conversely, given the statement datum $(G, D, G(\mathbb{R})^+ \to Hol(D)^+)$. We can obtain a decomposition of $G^{ad}_{\mathbb{R}} = H_1 \times \cdots \times H_2$ in simple factors. Let denote by H_c the product of the compact factors and H_{nc} the product of non compact factors. The action of $G(\mathbb{R})^+$ on D defines an isomorphism

$$H_{nc}(\mathbb{R})^+ \simeq Hol(D)^+$$

We can observe that we only use the non compact part because the lemma 2.2.5 shows us that if U_i is compact then the projection of u into this factor will be 1. Also, the set $\{u_p \ s.t \ p \in D\}$ is a $H_{nc}(\mathbb{R})^+-$conjugacy class of homomorphisms $U_1 \to H_{nc}(\mathbb{R})^+$ satisfying the first two Shimura axioms, due to [6, prop. 1.21]. Then we can define

$$\{(1, u_p) : \ S^1 \to H_c(\mathbb{R}) \times H_{nc}(\mathbb{R}) \ s.t \ p \in D\}$$

the $G^{ad}(\mathbb{R})^+-$conjugacy class of homomorphisms $S^1 \to G^{ad}(\mathbb{R})$ satisfying the first two Shimura axioms ∎

Observation 2.2.7. *Using the previous proposition, we know that a Shimura datum is very similar to a modular curve. We have an Hermitian symmetric domain that, as we have explained in the previous section, it is very similar to a piece of $\mathcal{H}^+$, and a group which acts on $\mathcal{H}^+$, in this case GL. The only piece that we lack is the congruence subgroup. As we have seen in the first chapter, defining congruence subgroups requires an elaborated argument. In the following theory, we will define what are congruence subgroups for this datum, giving us the complete generalization of modular curves, Shimura varieties.*

Given (G, D) a connected Shimura datum, we can define a *Shimura variety*. First, we are going to give some ideas that makes this definition consistent.

As proposition 2.2.6 said, if we have a Shimura datum, we have an hermitian symmetric domain D such that $G(\mathbb{R})^+$ acts on it. The construction of this action is given by the proof of that proposition. The map $G^{ad}(\mathbb{R})^+ \to Hol(D)^+$ has compact kernel, then, using the following chain

$$G^{ad}(\mathbb{Q})^+ \to G^{ad}(\mathbb{R})^+ \to Hol(D)^+$$

we have the definition of arithmetic subgroups of $Hol(D)^+$. Thus we can transfer arithmetic subgroups of $G^{ad}(\mathbb{Q})$ to $Hol(D)^+$ via this map, and it can be deduced that the kernel of $\Gamma \to \overline{\Gamma}$ is finite.
If $\overline{\Gamma}$ is torsion free, using the Borel theorem 1.3.29 we can construct $D(\Gamma) = \Gamma \setminus D$, which is a smooth Zariski-open subset of a projective algebraic variety. Then, as we said in the last section, using Chow's theorem, we can conclude that its compactification is an algebraic variety.
We observe that given a Shimura datum (G, D) we can construct a lot of different algebraic varieties. We will have two definitions of Shimura varieties, the "local" definition, which describes quotient varieties, and the "global" definition, which evolves all the information of a given Shimura datum.

Definition 2.2.8. Let (G, D) be a *connected Shimura datum*. A *connected Shimura variety* relative to (G, D) is an algebraic variety of the form $D(\Gamma)$ with Γ an arithmetic subgroup of $G^{ad}(\mathbb{Q})^+$ containing the image of a congruence subgroup of $G(\mathbb{Q})^+$ and such that $\overline{\Gamma}$ is torsion-free. The inverse system of such algebraic varieties, denoted by $Sh^o(G, D)$ is called the *connected Shimura variety* attached to (G, D).

Now, we want to construct a Shimura variety given a Shimura datum (G, D). As we can see, the only obstruction in the definition is how to obtain an arithmetic subgroup of $G^{ad}(\mathbb{Q})^+$ such that contains the image of a congruence subgroup of $G(\mathbb{Q})^+$. In order to solve this, we have a criterion given by the following two propositions

Proposition 2.2.9. *Let G be a reductive group over $\mathbb{Q}$. For any compact open subgroup $K \subset G(\mathbb{A}_f)$, then $K \cap G(\mathbb{Q})$ is a congruence subgroup of $G(\mathbb{Q})$.*

Proof. We can find this proof in [9, prop 2.2.2], and it is an easy exercise about algebraic groups. ∎

Proposition 2.2.10. *Let $\pi : G(\mathbb{Q})^+ \to G^{ad}(\mathbb{Q})^+$. The following conditions on an arithmetic subgroup Γ of $G^{ad}(\mathbb{Q})^+$ are equivalent:*

1. *$\pi^{-1}(\Gamma)$ is a congruence subgroup of $G(\mathbb{Q})^+$.*

2. *$\pi^{-1}(\Gamma)$ contains a congruence subgroup of $G(\mathbb{Q})^+$.*

3. *Γ contains the image of a congruence subgroup of $G(\mathbb{Q})^+$.*

Proof. $(1 \Rightarrow 2)$ Trivial by definitions.
$(2 \Rightarrow 3)$ Let Γ' be a congruence subgroup of $G(\mathbb{Q})^+$ contained in $\pi^{-1}(\Gamma)$. Then we have that

$$\Gamma \supset \pi(\pi^{-1}(\Gamma)) \supset \pi(\Gamma')$$

$(3 \Rightarrow 1)$ Let Γ' be a congruence subgroup of $G(\mathbb{Q})^+$ such that $\Gamma \supset \pi(\Gamma')$, we consider

$$\pi^{-1}(\Gamma) \supset \pi^{-1}\pi(\Gamma') \supset \Gamma'$$

Using that $\pi(\Gamma')$ is arithmetic [6, prop. 3.2], then it is of finite index in $\pi^{-1}(\Gamma)$. Let Z be the centre of G. We have that $Z(\mathbb{Q})\Gamma' \supset \pi^{-1}\pi(\Gamma')$, $Z(\mathbb{Q})$ is finite and Γ' is of finite index in $\pi^{-1}(\Gamma)$, proving that $\pi^{-1}(\Gamma)$ is a congruence subgroup. ∎

Observation 2.2.11. *The homomorphism $\pi : G(\mathbb{Q})^+ \to G^{ad}(\mathbb{Q})^+$ is usually not injective. Then, $\pi\pi^{-1}(\Gamma)$ is normally not equal to Γ. This implies that the family $D(\Gamma)$ with Γ congruence subgroup of $G(\mathbb{Q})^+$ is usually much smaller than $Sh^o(G, D)$.*

Proposition 2.2.12. *Let (G, D) be a connected Shimura datum with G simply connected. Let K be a compact open subgroup of $G(\mathbb{A}_f)$, and let $\Gamma = K \cap G(\mathbb{Q})$ be the corresponding congruence subgroup of $G(\mathbb{Q})$. The map $x \to (x, 1)$ defines the bijection*

$$\Gamma \setminus D \simeq G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$$

Here, the action is defined as follows

- *$G(\mathbb{Q})$ acts on both D and $G(\mathbb{A}_f)$ on the left, i.e, $q \cdot (x, a) = (qx, qa)$.*

- *K acts only on $G(\mathbb{A}_f)$ on the right, i.e, $(x, a) \cdot k = (x, ak)$.*

If we endow D with its usual topology and $G(\mathbb{A}_f)$ with the adelic topology, this becomes an homeomorphism.

Proof. Using 2.1.8, we can express $G(\mathbb{A}_f) = G(\mathbb{Q})K$. Then we can express every element of $G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$ as $[x, 1]$. Using the definition of our coset, we have that

$$[x, 1] = [x', 1] \textit{ if and only if there exist } q \in G(\mathbb{Q}) \textit{and } k \in K \textit{ such that } x' = qx,\ 1 = qk$$

Since $k \in K$, $q \in G(\mathbb{Q})$ and $q = k^{-1}$, we have that $a = k^{-1} \in G(\mathbb{Q}) \cap K = \Gamma$. Thus, $[x,1] = [x',1]$ if and only if x and x' represent the same element in $\Gamma \setminus D$. Consider the following diagram

$$\begin{array}{ccc} D & \xrightarrow{x \to (x,[1])} & D \times (G(\mathbb{A}_f)/K) \\ \downarrow & & \downarrow \\ \Gamma \setminus D & \xrightarrow{[x] \to [x,1]} & G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K \end{array}$$

Using that K is open, then $G(\mathbb{A}_f)/K$ is discrete, and then the upper map is an homeomorphism. The lower map is an homeomorphism by definition of our coset. ∎

At first sight, the expression $\Gamma \setminus D$ seems to be easier than $G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$, but the latter expression allows us to construct $Sh^o(G,D)$. Before constructing $Sh^o(G,D)$, we need to prove an auxiliar lemma.

Lemma 2.2.13. *Lets G be a topological group acting continuously on a topological space X. Let $(G_i)_{i \in I}$ be a directed family of subgroups of G.*

1. *The canonical map $h : X/\cap G_i \to \varprojlim X/G_i$ is continuous.*
2. *The map h is injective if the stabilizer in G_i of x is compact for every $x \in X$ and $i \in I$.*
3. *The map h is surjective if the orbit xG_i is compact for every $x \in X$ and $i \in I$.*

Proof. In this proof we will use the fact that a direct intersection of non empty compact sets is nonempty. Then we have that a directed inverse limit of nonempty compact sect is non-empty.

1. Let $I = \bigcap G_i$. We know that I acts continuously on X, and the map
$$X/I \to X/G_i$$
is continuous for every i. Then the inverse limit of these continuous maps is continuous.
2. Let $x, x' \in X$. For each i, we define
$$G_i(x,x') = \{g \in G_i \ s.t \ xg = x'\}$$
By the hypothesis $G_i(x,x')$ is compact. Also, if x and x' have the same image in the inverse limit $\varprojlim X/G_i$, then $G_i(x,x')$ is non empty for those x, x'. Then, the intersection of those sets is non empty.
Lets g be in the intersection, lets $xg = x'$. This shows that x and x' have the same image in $X/\cap G_i$, proving us the statement.
3. Let $(x_iG_i)_{i \in I} \in \varprojlim X/G_i$. Since each orbit is compact $\varprojlim x_iG_i$ is non empty. Then if $x \in \varprojlim x_iG_i$, then $x \cap G_i$ maps to $(x_iG_i)_{i \in I}$.

∎

Observation 2.2.14. *The conclusions of the lemma hold if every subgroup G_i is compact and every orbit xG_i is Hausdorff.*

Proposition 2.2.15. *We have the following expression*

$$\varprojlim_K G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K = G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)$$

Proof. Lets $(x,a) \in D \times G(\mathbb{A}_f)$ and lets K be a compact open subgroup of $G(\mathbb{A}_f)$. To use the previous proposition, we have to check that the image of the orbit $(x,a)K$ in $G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)$ is Hausdorff for K sufficiently small.
Lets $\Gamma = G(\mathbb{Q}) \cap aKa^{-1}$. We can assume that Γ is torsion free. Then there exists an open

neighborhood V of x such that $gV \cap V = \varnothing$ for all $g \in \Gamma \setminus \{1\}$. Let suppose that for any $(x,b) \in (x,a)K$, we have that $g(V \times aK) \cap (V \times bK) \neq \varnothing$ for $g \in G(\mathbb{Q})$. Then we have that

$$gaK = bK = aK$$

Applying this result, we obtain that $g \in G(\mathbb{Q}) \cap aKa^{-1} = \Gamma$. Using that $gV \cap V \neq \varnothing$, we deduce that $g = 1$, and then we can assert that

$$g(V \times aK) \cap (V \times bK) = \varnothing$$

for all $g \in G(\mathbb{Q}) \setminus \{1\}$. Then the images of $V \times Ka$ and $V \times Kb$ in $G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)$ separate (x,a) and (x,b). We can apply the last lemma, obtaining a bijective map between those two sets. ∎

We can give an alternative definition of Shimura datum. This will help us to define what is a *non-connected Shimura variety.*

We have an exact sequence of Lie groups as follows

$$0 \to \mathbb{R} \xrightarrow{r \to r^{-1}} \mathbb{C}^* \xrightarrow{z \to z/\overline{z}} S^1 \to 0$$

This arises from this general exact sequence

$$0 \to \mathbb{G}_m \xrightarrow{\omega} \mathbb{S} \to U_1 \to 0$$

where $\mathbb{S} = Res_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$ and $U_1 = \mathbb{S}/\mathbb{G}_m$ (and ω defined such that the restriction is the inverse map; this map is called *the weight homomorphism* and will be defined in 2.2.20). Those two sequences are related by its definition, since $\mathbb{G}_m(\mathbb{R}) = \mathbb{R}^*$ and $\mathbb{S}(\mathbb{R}) = \mathbb{C}^*$. This exact chain allows us to make a more general definition of what is a Shimura datum. Given a Shimura datum (G, D), we have a map $u : S^1 \to G$. This map defines an homomorphism $h : \mathbb{S} \to G$ using the following definition

$$h(z) = u(z/\overline{z})$$

By definition, S^1 acts on $Lie(G)_\mathbb{C}$ through the characters $z, 1, z^{-1}$ if and only if $\mathbb{S}$ acts on $Lie(G)_\mathbb{C}$ through the characters $z/\overline{z}, 1, \overline{z}/z$. Implication "$\Rightarrow$" is obvious by the definition of h. Conversely, lets $h : \mathbb{S} \to G$ an homomorphism for which $\mathbb{S}$ acts on $Lie(G)_\mathbb{C}$ through the characters $z/\overline{z}, 1, \overline{z}/z$. $\omega(\mathbb{G}_m)$ acts trivially on $Lie(H)_\mathbb{C}$ since $w(\mathbb{G}_m) = ker(z/\overline{z})$. This is because the above sequence is exact. Then, we obtain that h is trivial on $\omega(\mathbb{G}_m)$. We conclude that h arises from a u, giving us the desired result.

The notation that we are going to follow is the same as in the first chapter, lets G be a reductive group over $\mathbb{Q}$, lets $G^{ad} = G/Z(G)$. We are going to denote by $G(\mathbb{R})_+$ the group of elements of $G(\mathbb{R})$ whose image in $G^{ad}(\mathbb{R})$ lies in $G^{ad}(\mathbb{R})^+$. Also we are going to denote by $G(\mathbb{R})_+ = G(\mathbb{Q}) \cap G(\mathbb{R})_+$.

Definition 2.2.16 (Alternative definition of connected Shimura datum)**.** A *connected Shimura datum* can be alternatively defined as a pair $(G, D = \{h\})$, where G and D are as in the first definition, except that

$$h : \mathbb{S}_\mathbb{R} \to G^{ad}_\mathbb{R}$$

is an homomorphism of real algebraic groups satisfying the conditions

- *SV1:* Only the characters 1, $z/\overline{z}$ and $\overline{z}/z$ occur in the representation of $\mathbb{S}_\mathbb{R}$ on $Lie(G^{ad})_\mathbb{C}$.
- *SV2:* $Ad(h(i))$ is a Cartan involution on $Lie(G^{ad}_\mathbb{R})$.
- *SV3:* There exists no factor H of G^{ad} over $\mathbb{Q}$ such that $H(\mathbb{R})$ is compact.

Continuing with this approach, we can define the general *Shimura datum*

Definition 2.2.17. A *Shimura datum* is a pair (G, D) consisting of a reductive group G over $\mathbb{Q}$ and a $G(\mathbb{R})-$conjugacy class D of homomorphisms $h: \mathbb{S} \to G_{\mathbb{R}}$ satisfying the following conditions:

- *SV1:* For all $h \in D$, only the characters 1, $z/\overline{z}$ and $\overline{z}/z$ occur in the representation of $\mathbb{S}_{\mathbb{R}}$ on $Lie(G_{\mathbb{R}})$.
- *SV2:* for all $h \in D$, $ad(h(i))$ is a Cartan involution of $G^{ad}_{\mathbb{R}}$.
- *SV3:* G^{ad} has no $\mathbb{Q}-$factor on which the projection of h is trivial.

Observation 2.2.18. *The differences between a connected Shimura datum and a (possible) non connected Shimura datum are:*

- *In a general Shimura datum G is reductive, in contrast to a connected Shimura datum, in which G is semisimple.*
- *In a general Shimura datum h arrives to $G_{\mathbb{R}}$, however, in a connected Shimura datum, h has target G^{ad}.*

The latter difference is the one that gives the name "connected".

Examples 2.2.19.

- *Let $G = SL_2$ and $D = \mathcal{H}_1$. Then $Sh(G, D)$ is the family of modular curves $\mathcal{H}_1/\Gamma$ with Γ a torsion free arithmetic subgroup of PGL_2 containing the image of $\Gamma(N)$ for some N.*
- *Lets $G = T$ be a torus over $\mathbb{Q}$, let's choose any morphism $h: \mathbb{S} \to T$. Since a torus is conmutative, $T^{ad} = \{1\}$. The Shimura conditions holds. Lets $D = \{x\}$ be a single point. For any compact open subgroup $K \subset G(\mathbb{A}_f)$, we have that*

$$Sh_K(T, x) = T(\mathbb{Q}) \setminus \{x\} \times T(\mathbb{A}_f)/K \simeq T(\mathbb{Q}) \setminus T(\mathbb{A}_f)/K$$

is a finite set of points by 2.1.5.

Definition 2.2.20. Lets (G, D) be a Shimura datum, for every $h: \mathbb{S} \to G_{\mathbb{R}}$ in X, we define the *weight homomorphism* as

$$\begin{aligned} \omega : \mathbb{G}_{m,\mathbb{R}} &\to G_{\mathbb{R}} \\ z &\to 1/h(z) \end{aligned}$$

Proposition 2.2.21. *The weight homomorphism is unique and it is well defined.*

Proof. A priori, we could think that the weight homomorphism depends on the election of h. What we are going to prove is that, given a Shimura datum, taking any $h \in D$, we obtain the same weight homomorphism ω.

Every $h: \mathbb{S} \to G_{\mathbb{R}}$ in D acts on $Lie(G)_{\mathbb{C}}$ with characters $z/\overline{z}, 1, \overline{z}/z$ (due to the composition with Ad). Using the definition of h, $h(z) = u(z/\overline{z})$, we can see that $h|_{\mathbb{G}_{m,\mathbb{R}}=\mathbb{R}^*} = id$, and then $h(r)$ must acts trivially on $Lie(G_{\mathbb{R}})_{\mathbb{C}}$ for any $r \in \mathbb{R}$. As we know, the only elements of $G(\mathbb{R})$ that act trivially are those that are in the center of G, and then $h(r) \in Z(G)$ for all $r \in \mathbb{R}$. Hence, $h|_{\mathbb{G}_{m,\mathbb{R}}}$ does not depend on the election of h. This is because all the elements of D are $G(\mathbb{R})-$conjugated This implies that given $h' \in D$, $h' = ghg^{-1}$ for some $g \in G(\mathbb{R})$, using the fact that $h(r) \in Z(G)$, we obtain

$$h'(r) = gh(r)g^{-1} = gg^{-1}h(r) = h(r)$$

∎

The following proposition will relate connected Shimura datum with Shimura datum, and allows us to translate results of connected Shimura datums to results of general Shimura datums.

Proposition 2.2.22. *Lets G be a reductive group over $\mathbb{R}$. Lets $h: \mathbb{S} \to G$ be an homomorphism. Let's define $\overline{h}: \mathbb{S} \xrightarrow{h} G \xrightarrow{/Z(G)} G^{ad}$. Lets D be a $G(\mathbb{R})-$conjugacy class of homomorphisms $\mathbb{S} \to G$, and $\overline{D}$ be the $G^{ad}(\mathbb{R})-$conjugacy class of homomorphisms $\mathbb{S} \to G^{ad}$ containing $\overline{h}$ for $h \in D$.*

1. *The following map*

$$\begin{aligned} D &\to \overline{D} \\ h &\to \overline{h} \end{aligned}$$

   is injective. Its image is the union of connected components of $\overline{D}$.

2. *Lets D^+ be a connected component of D. Lets $\overline{D}^+$ be its image in $\overline{D}$ by the previous map. If (G, D) satisfies the first three Shimura axioms, then $(G^{der}, \overline{D}^+)$ satisfies the first three Shimura axioms. Also, the stabilizer of D^+ in $G(\mathbb{R})$ is $G(\mathbb{R})_+$, i.e, $gX^+ = X^+ \iff g \in G(\mathbb{R})_+$.*

Proof. 1. This proof can be found in [6, prop. 5.7]. To prove the injectivity uses the fact that we can determine an homomorphism $\mathbb{S} \to G$ by its projections to G^{der} and to the bigger commutative quotient of G. To prove the second part of the statement, we use that $G^{ad}(\mathbb{R})^+$ acts transitively on each connected component of $\overline{D}$ by [6, prop. 1.5]. Then $G(\mathbb{R})^+ \to G^{ad}(\mathbb{R})^+$ is surjective.

2. The first part is trivial, and the second part can be found at [6, prop. 5.7], whose proof uses algebraic groups theory.

∎

Proposition 2.2.23. *Lets (G, D) be a Shimura datum. For every connected component D^+ of D,*

$$G(\mathbb{Q})_+ \setminus D^+ \times G(\mathbb{A}_f) \to G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)$$

is a bijection

Proof. Using proposition 2.1.9, we know that $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$. Also, $G(\mathbb{R})$ acts on D^+ as the automorphism group of D. We know that D is a hermitian symmetric domain. Using the definition 1.3.12 and [6, prop. 1.5], we know that $G^{ad}(\mathbb{R})^+$ acts transitively on each component of X. Since $G(\mathbb{R}) \to G^+(\mathbb{R}) \to G^{ad}(\mathbb{R})^+$ is surjective, then $G(\mathbb{R})$ acts transitively on D, i.e, the action has only one orbit. Thus, we can express every $x \in D$ as $x = qx^+$, with $q \in G(\mathbb{Q})$ and $x^+ \in D^+$. Then, we have deduced that the statement map is surjective.
Let (x, a) and (x', a') be elements of $D^+ \times G(\mathbb{A}_f)$. If $[x, a] = [x', a']$ in $G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)$, then by definition we have

$$x' = qx, \quad a' = qa, \quad \textit{with } q \in G(\mathbb{Q})$$

Since x and x' are in D^+, the element q stabilizes D^+, and then by 2.2.23 lies in $G(\mathbb{R})^+$. We can conclude that $[x, a] = [x', a']$ in $G(\mathbb{Q})_+ \setminus D \times G(\mathbb{A}_f)$. ∎

Proposition 2.2.24. *Lets (G, D) be a Shimura datum. Lets D^+ be a connected component of D and $K \subset G(\mathbb{A}_f)$ be a compact open subgroup. Then*

1. *$G(\mathbb{Q})^+ \setminus G(\mathbb{A}_f)/K$ is finite as a set. Lets $\mathfrak{C}$ be the set of representatives of the double coset.*

2. *There exists an homeomorphism*

$$\begin{aligned} \cup_{c \in \mathfrak{C}} \Gamma_c \setminus D^+ &\to G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K \\ x &\to (x, c_x) \end{aligned}$$

   where $\Gamma_c = cKc^{-1} \cap G(\mathbb{Q})_0$ and c_x denotes the connected component to which x belongs.

Proof. 1. Using the proposition [6, prop. 5.3], we know that the group $G^{ad}(\mathbb{R})^+ \setminus G^{ad}(\mathbb{R})$ is finite. Also, we define the following map

$$G(\mathbb{Q})_+ \setminus G(\mathbb{Q}) \to G^{ad}(\mathbb{R})^+ \setminus G^{ad}(\mathbb{R})$$

that is injective because $G(\mathbb{Q})$ is reductive and then connected. It suffices to show that $G(\mathbb{Q}) \setminus G(\mathbb{A}_f)/K$ is finite. We have proved along this dissertation cases of this quotient, also we can find the general proof in [6, prop. 5.17].

2. Lets $g \in \mathfrak{C}$, consider the map

$$\begin{aligned} \Gamma_g \setminus D^+ &\to G(\mathbb{Q})_+ \setminus D^+ \times G(\mathbb{A}_f)/K \\ [x] &\to [x, g] \end{aligned}$$

This map, for each g is injective. This is because if $[x, g] = [x', g]$, then $x' = qx$ and $g = qgk$ for some $q \in G(\mathbb{Q})_+$ and $k \in K$. Thus we have found that $q \in \Gamma_g$, and then $[x] = [x']$.

Also we say that $G(\mathbb{Q})_+ \setminus D^+ \times G(\mathbb{A}_f)/K$ is the disjoint union of images of these maps if we change g. To prove this, lets $(x, a) \in G(\mathbb{A}_f)$. Then $a = qgk$ for some $q \in G(\mathbb{Q})_+$, $g \in \mathfrak{C}$ and $k \in K$. Then $[x, a] = [q^{-1}x, g]$, which lies in the image of $\Gamma_g \setminus D^+$. Now we suppose that $[x, g] = [x', g']$, with $g, g' \in \mathfrak{C}$. Then we have that $x' = qx$ and $g' = qgk$ for some $q \in G(\mathbb{Q})_+$ and $k \in K$. This implies that $g' = g$.

Then, we can see that the map of the statement is an homeomorphism using 2.2.23.

∎

Definition 2.2.25. Lets (G, D) be a Shimura datum. A *Shimura variety* is defined as

$$Sh(G, D) = \varprojlim_K G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$$

where K runs among compact open subgroups of $G(\mathbb{A}_f)$ such that the image of all congruence subgroups $\Gamma_c = cKc^{-1} \cap G(\mathbb{Q})_0 \subset G(\mathbb{Q})$ in $G^{ad}(\mathbb{Q})$ are torsion free.

Observation 2.2.26. *We can define an action of $G(\mathbb{A}_f)$ in $Sh(G, D)$ as follows: If $g = \{g_l\} \in G(\mathbb{A}_f)$ we have the homomorphism*

$$\begin{aligned} T_g : \ Sh_K(D, G) &\to Sh_{g^{-1}Kg}(D, G) \\ (x, a) &\to (x, ag) \end{aligned}$$

This action induces a permutation over the set of representatives of this double coset.

As in every field of mathematics, when we define an object, we must define the maps with good behaviour between them. In this case we have Shimura varieties morphisms, which respects the structures of the Shimura datum.

Definition 2.2.27. Let (G, X) and (G', X') be Shimura data

- A *morphism of Shimura data* $(G, X) \to (G', X')$ is a homomorphism $G \to G'$ of algebraic groups sending X to X'.
- A *morphism of Shimura varieties* $Sh(G, X) \to Sh(G', X')$ is an inverse system of regular maps of algebraic varieties compatible with the action of $G(\mathbb{A}_f)$.

Theorem 2.2.28. *A morphism of Shimura data $(G, X) \to (G', X')$ defines a morphism $Sh(G, X) \to Sh(G', X')$ of Shimura varieties which is a closed immersion if $G \to G'$ is injective*

We can prove the first part of the theorem by Borel's theorem 1.3.29. The second part of the proof can be found in [5, thm. 1.15].

2.3 Moduli interpretation

Since Shimura varieties are the generalization of modular curves, it seems logical that some Shimura variety has a modular interpretation. This geometric objects parametrize families of abelian varieties, giving us a more general vision of these objects. As we will see, we will construct a Shimura variety which classifies some family of abelian varieties, the *Siegel modular variety*, and successively, we will construct finer spaces to classify more specific families.

In order to define the *Siegel modular variety*, we have to introduce new concepts. To explain those ideas, as an example, we will define a Shimura datum in terms of a Simplectic group. That will give us the ideas about how can we generalize this construction.

From the classic theory about modular forms, we know that $SL_2(\mathbb{R}) \circlearrowleft \mathcal{H}$ with Moebius transformations. Then, we can write

$$\mathcal{H}_1 = SL_2(\mathbb{R})i$$

And then, using that the isotropy group for i is $SO_2(\mathbb{R})$, we can express

$$\mathcal{H}_1 \simeq SL_2(\mathbb{R})/SO_2(\mathbb{R})$$

We can generalize the complex half plane defining the *Siegel half plane*

$$\mathcal{H}_n = \{Z \in M_n(\mathbb{C}) \ s.t\ Z^t = Z,\ Im(Z) \geq\}$$

The group which acts on this space is

$$Sp_{2n}(\mathbb{R}) = \{g \in GL_{2n}(\mathbb{R}) \ s.t\ g^t\psi_n g = \psi_n\}$$

with $\psi_n = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}$ the symplectic matrix. Lets $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2n}(\mathbb{R})$ and $Z \in \mathcal{H}_n$, the action is defined as

$$gZ = (AZ + B)(CZ + D)^{-1}$$

This is a transitive action. Using the fact that the stabilizer of iI_n is $U_n = \left\{\begin{pmatrix} A & B \\ -B & A \end{pmatrix} \in Sp_{2n}\right\}$, we can express

$$\mathcal{H}_n = Sp_{2n}(\mathbb{R})/U_n$$

We can interpret this result as a Shimura datum.
Lets $G = Sp_{2n}$ defined over $\mathbb{Q}$, it is semisimple. We define

$$h_0 :\ U_1 \to G^{ad}_{\mathbb{R}} = G_{\mathbb{R}} \setminus \{\pm Id\}$$
$$x + iy \to \begin{pmatrix} xI_n & -yI_n \\ yI_n & xI_n \end{pmatrix}$$

We set $D = \{G(\mathbb{R})-\textit{conjugacy class of } h_0\} = Sp_{2n}(\mathbb{R})h_0$. We can also deduce that $Cent_{h_0}(Sp_{2n}(\mathbb{R})) = U_n$, and then we can express

$$\mathcal{H}_n = Sp_{2n}h_0$$

with the action given by conjugation. Then $(Sp_{2n}, \mathcal{H}_n)$ is a connected Shimura datum. This Shimura datum is an example of how can we construct a Shimura datum from a given symplectic group. The aim of this section will be to generalize this Shimura variety.

Lets (V, ψ) be a symplectic space of dimension $2n$ (there are no symplectic spaces of odd dimension). That is, V a vector space over $\mathbb{Q}$ and ψ an alternating, non degenerate bilinear form $\psi :\ V \times V \to \mathbb{Q}$ (symplectic form). Using the fact that every symplectic form is defined by a

skew-symmetric matrix, we can find a basis of V such that $\psi = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
We define $G = GSp(V, \psi)$ over $\mathbb{Q}$ as

$$G(\mathbb{Q}) = \{g \in GL(V) \ s.t \ \psi(gu, gv) = \nu(g)\psi(u, v)\}$$

with $\nu(g) \in \mathbb{Q}^*$. This group induces a homomorphism $\nu : \ G \to \mathbb{G}_m$.

Observation 2.3.1. *The map ψ satisfies the following property*

$$\psi(Ju, Jv) = \psi(u, v)$$

Observation 2.3.2. *Using the fact that $\psi(gu, gv)$ can be written as $(gu)^t\psi_n(gv) = u^t g^t \psi_n gv$, we obtain that $S = Sp_{2n} = ker(\nu)$. And then, we have that $Sp_{2n} \subset G$.*

A symplectic complex structure J on $(V(\mathbb{R}), \psi)$ is an endomorphism $J \in S(\mathbb{R})$ such that $J \neq Id$, $J^2 = -Id$. Using this structure and defining $J(v) = iv$ for all $v \in V$, we can define V as a complex vectorial space. We define the following bilinear form

$$\begin{aligned} \psi_J : \ V(\mathbb{R}) \times V(\mathbb{R}) &\to \mathbb{R} \\ (u, v) &\to \psi(u, Jv) \end{aligned}$$

This bilinear form is symmetric. We say that a complex structure is *positive* if ψ_J is positive (respectively *negative*).
We define $D = \{$*positive and negative symplectic complex structures on* $V(\mathbb{R})\}$. We can divide D as $D = D^+ \cup D^-$. The group $G(\mathbb{R})$ acts on D by conjugation, i.e

$$(g, J) \to gJg^{-1}$$

The stabilizer of D^+ in $G(\mathbb{R})$ is $G(\mathbb{R})_0 = \{g \in G(\mathbb{R}) \ s.t \ \nu(g) > 0\}$. Also, $G(\mathbb{R})$ acts transitively on D and $S(\mathbb{R})$ acts transitively on D^+.
We can associate to each $J \in D$ a morphism as follows

$$\begin{aligned} h_J : \ \mathbb{C}^* &\to G(\mathbb{R}) \\ a + bi &\to a + bJ \end{aligned}$$

We can understand $a + bJ \in G(\mathbb{R})$ as $aI_n + biI_n$. Using the fact that $h_{gJg^{-1}} = gh_J g^{-1}$ for any $g \in G(\mathbb{R})$, we identify

$$D \longleftrightarrow \{G(\mathbb{R}) - \textit{conjugation class of } h_J : \ \mathbb{C}^* \to G(\mathbb{R})\}$$

Lemma 2.3.3. *Lets V be a vector space over $\mathbb{R}$, if we have a complex structure J, then*

1. *J has $\pm i$ eigenvalues.*
2. *We can decompose $V(\mathbb{C}) = V^+ \oplus V^-$.*

Proof. This vector space is the "realization" of some complex vector space, because we have a complex structure. We have the following homomorphism

$$\begin{aligned} u : \ V_{\mathbb{C}} &\to V(\mathbb{C}) \oplus \overline{V}(\mathbb{C}) \\ v \otimes z &\to (zv, \overline{z}v) \end{aligned}$$

with $V(\mathbb{C})$ and $\overline{V}(\mathbb{C})$ being the same group. Also we have the property that iv (using i as the endomorphism J) in $\overline{V}(\mathbb{C})$ is equal to $-iv$.
Since we can not express every element of $V_{\mathbb{C}}$ as $a \otimes b$, for those elements of the form $a \otimes b + c \otimes d$

this map is defined as $u(a \otimes b + c \otimes d) = u(a \otimes b) + u(c \otimes d)$. Then, this map is an isomorphism. We define subspaces as follows

$$V_{\mathbb{C}}^{(1,0)} = \{v \otimes 1 - iv \otimes i \ s.t \ v \in V\}, \quad V_{\mathbb{C}}^{(0,1)} = \{v \otimes 1 + iv \otimes i \ s.t; v \in V\}$$

Then we have a decomposition of $V_{\mathbb{C}}$ as the direct sum of those subspaces. To prove this, we need to show that every element of $V_{\mathbb{C}}$ can be written as the sum of elements which belong to those subspaces. Using the properties of the tensor product, we only need to prove this fact for

$$v \otimes 1 + w \otimes i = (\frac{v+iw}{2} \otimes 1 - i\frac{v+iw}{2} \otimes i) + (\frac{v-iw}{2} \otimes 1 + i\frac{v-iw}{2} \otimes i)$$

As we can divide the vector space with those spaces, and in those spaces J acts like the multiplication by i or $-i$, J has these eigenvalues.

∎

Proposition 2.3.4. *(G, D) satisfies the axioms of being Shimura datum.*

Proof.

1. **SV1**: Since J is an endomorphism, we can decompose V in terms of its eigenvalues, as in the previous proposition
$$V(\mathbb{C}) = V^+ \oplus V^-$$
Then, the element $h(z)$ acts on V^+ as the multiplication by z, and on V^- as the multiplication by $\overline{z}$. Now, we need to understand how $Ad(h(z))$ acts on $Lie(G)_{\mathbb{C}}$. We have the following chain
$$\mathbb{C}^* \to G(\mathbb{R}) \xrightarrow{Ad} GL(Lie(G)_{\mathbb{C}}) \subset End(V(\mathbb{C}))$$
The map Ad acts by conjugation, i.e, $Ad(g)f = gfg^{-1}$. We can divide
$$End(V) = End(V^+) \oplus End(V^-) \oplus Hom(V^+, V^-) \oplus Hom(V^-, V^+)$$
For each $f \in Hom(V^+, V^-)$ we have that $Ad(h(z))(f) = h(z)fh(z)^{-1}$. Then, using the fact that $h(z)^{-1}$ acts on V^+ as the multiplication by z^{-1}, we have that $h(z)fh(z)^{-1}(v) = h(z)f(h(z)^-1v) = h(z)f(z^-1v)$. Now using that $Im(f) \subset V^-$ and $h(z)$ acts on V^- as the multiplication by $\overline{z}$, we have that
$$h(z)f(z^{-1}v) = \frac{\overline{z}}{z}f(v)$$
Applying this to all the possible cases we obtain that
$$\begin{array}{rcccc} & End(V^+) \oplus & Hom(V^+, V^-) \oplus & Hom(V^-, V^+) \oplus & End(V^-) \\ \textit{action of } ad(h(z)) \to & (1, & z/\overline{z}, & \overline{z}/z, & 1) \end{array}$$
The action of ad and Ad are the same, because $h(z) \in GL(\mathbb{R})$ and the derivative of a linear map is itself.

2. **SV2**: We need to prove that $Ad(h(i))$ is a Cartan involution on $LieG_{\mathbb{R}}^{ad}$. As in the previous proof, in our case $Ad = ad$. We have that
$$\begin{aligned} ad(h(i)): \ G^{ad}(\mathbb{R}) &\to G^{ad}(\mathbb{R}) \\ g &\to JgJ^{-1} \end{aligned}$$
Our map satisfies $ad(h(i)) \neq 1$, $ad(h(i))^2 = Id$. Its $+1-$eigenspace are fixed points of the map, that are
$$\{g \in G(\mathbb{R}) \ s.t \ Jg = gJ\} = \{g \in G(\mathbb{R}) \ s.t \ \psi_J(gu, gv) = \psi(u, v)\}$$
Using that ψ_J is positive definite, we conclude that this subgroup is compact.

3. **SV3**: We have that G^{ad} is simple over $\mathbb{Q}$ and $G^{ad}(\mathbb{R})$ itself is not compact.

∎

Definition 2.3.5. We define the *Siegel modular variety* attached to (V,ψ) to be a Shimura variety $Sh(G,D)$, with (G,D) as before.

As we said in the introduction of this section, the objective of those Shimura varieties is to define Moduli spaces of Abelian varieties.
Lets (G,D) be a Shimura datum defined by a symplectic space (V,ψ), and $K\subset G(\mathbb{A}_f)$ be an open compact subgroup. Lets $Sh_K(G,D) = G(\mathbb{Q})\setminus D\times G(\mathbb{A}_f)/K$. Lets $A/\mathbb{C}$ be a complex abelian variety of dimension n, then we can express $A=\mathbb{C}^n/\Lambda$ with Λ complex lattice. We define $V(\mathbb{R}) = \Lambda\otimes_{\mathbb{Z}}\mathbb{R}\simeq\mathbb{C}^n$. The last isomorphism transfers a complex structure to $V(\mathbb{R})$.

Definition 2.3.6. A polarization on A is a non-degenerate alternating form $s:\ \Lambda\times\Lambda\to\mathbb{Z}$ such that $s(Ju,Jv)=\psi(u,v)$ for all $u,v\in V(\mathbb{R})$, and $s_J(u,v)=s(u,Jv)$ is positive definite.

We can define $V(\mathbb{A}_f)=V(\mathbb{R})\otimes_{\mathbb{R}}\mathbb{A}_f=\Lambda\otimes_{\mathbb{Z}}\mathbb{R}\otimes_{\mathbb{R}}\mathbb{A}_f=\Lambda\otimes_{\mathbb{Z}}\mathbb{A}_f=\mathbb{A}_f^{2n}$. Also, we define the *Tate module* of A as $V_f(A)=H_1(A,\mathbb{A}_f)\simeq\Lambda\otimes\mathbb{A}_f$.

Lets $M_K(G,D)=\{A,s,\eta K\}$, where

- A is a complex abelian variety of dimension n such that $A(\mathbb{C})=V(\mathbb{R})/\Lambda$.
- s is an alternating form on $H_1(A,\mathbb{Z})$ such that s or $-s$ is a polarization on A.
- ηK is a $K-$orbit of $\mathbb{A}_f-$linear isomorphisms $\eta: V(\mathbb{A}_f)\xrightarrow{\simeq}V_f(A)$ such that $\eta_*(\psi)=as$ for some $a\in\mathbb{A}_f^*$. This is well defined since $G(\mathbb{A}_f)$ acts on $V(\mathbb{A}_f)$ with the action inherited from the action of $G(\mathbb{Q})$ on $V(\mathbb{R})$.

We say that two triples $(A,s,\eta K)$ and $(A',s',\eta' K)$ are isomorphic if there exists an isogeny $f:A\to A'$ such that $f^*(s')=qs$ with $q\in\mathbb{Q}^*$ and $f^*(\eta' K)=\eta K$.

Theorem 2.3.7. *The Shimura variety $Sh_K(G,D)$ is the coarse moduli space over $\mathbb{C}$ which classifies triples in $M_K(G,D)$ up to isomorphism. In particular, there is a canonical bijection between*

$$M_K(G,D)/\simeq\longleftrightarrow G(\mathbb{Q})\setminus D\times G(\mathbb{A}_f)/K$$

We can read this proof in [6, p. 60]. Its proof uses that Siegel modular varieties also parametrize other objects (Hodge structures). The correspondence between this Shimura variety and Hodge structures is simple, then, using Riemann's Theorem, which relates abelian varieties with Hodge structures, we are done.
Although, without the proof, we may deduce a correspondence like that of the statement. In one side we have abelian varieties, which we can be expressed as the quotient of a vector space, polarizations of this abelian variety, that are very similar to symplectic forms. The last element determine the level structure of the Shimura curve, and it is defined with the isomorphism that we have used defining $V(\mathbb{A}_f)$ above.

Now we are going to define other Shimura variety (which will solve a moduli problem) using the Siegel modular variety. We are going to study Shimura varieties of *Hodge type*. Before defining this new object, we must introduce new concepts.

Definition 2.3.8. A *Hodge structure* is a real vector space V together with a decomposition of $V(\mathbb{C})$ into complex vector subspaces of the following form

$$V(\mathbb{C})=\oplus V^{p,q},\ \ s.t\ \ (p,q)\in\mathbb{Z}\times\mathbb{Z}\ \ with\ \ \overline{V}^{p,q}=V^{q,p}$$

We define the *type* of a Hodge structure as the set of pairs (p,q) for which $V^{p,q}\neq 0$

Given a Hodge structure, its *weight decomposition* is the following

$$V = \bigoplus_{n\in\mathbb{Z}} V_n$$

where V_n is the real vector subspace of V such that $V_n(\mathbb{C}) = \bigoplus_{p+q=n} V^{p,q}$. If $V = V_n$, we say that is a Hodge structure of weight n.
We define a *rational* Hodge structure as a vector space over $\mathbb{Q}$ with a Hodge structure for $V(\mathbb{R})$, with V_n defined over $\mathbb{Q}$ for all $n \in \mathbb{Z}$.

Examples 2.3.9.

- *When we proved that a symplectic datum is a Shimura datum at 2.3.4, we gave a Hodge decomposition in terms of eigenspaces of J. This is because, as we proved in 2.3.3, to give a complex structure J on V real vector space, is equivalent to give a Hodge structure*
$$V(\mathbb{C}) = V^{-1,0} \oplus V^{0,-1}$$
- *Lets X be a non-singular projective variety. Lets $V = H^n(X,\mathbb{Q})$, this is a vector space over $\mathbb{Q}$. We need to express our vector space over $\mathbb{C}$. We can do this by tensor product, i.e, $V(\mathbb{C}) = H^n(X,\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = H^n(X,\mathbb{C})$. Using the de Rahm's theorem, we can compute this cohomology using de Rahm cohomology, then $V(\mathbb{C}) = H^n_{dR}(X,\Omega^n)$, where Ω^n are differential $n-$forms. We can see this $n-$forms as the exterior product between a $p-$form and a $m-$form such that $p+m=n$. Then we can write*
$$V(\mathbb{C}) = \bigoplus_{p+m=n} H^m(X,\Omega^p)$$

Definition 2.3.10. We define *morphisms of Hodge structures* as maps

$$t:\ V = \bigoplus_{(p,q)} V^{p,q} \to W = \bigoplus_{(p,q)} W^{p,q}$$

that are linear and satisfy $t(V^{p,q}) \subseteq W^{p,q}$.

Definition 2.3.11. A Shimura datum (G,D) is of *Hodge type* if there exists a symplectic vector space (V,ψ) over $\mathbb{Q}$ and a monomorphism $G \hookrightarrow GS_p(V,\psi)$ such that D maps to $D_{(V,\psi)}$. The Shimura variety $Sh(G,D)$ is called of *Hodge type*.

We can define the character $\nu : GS_p(V,\psi) \to \mathbb{G}_m$ at G (using the inclusion). Then, we are going to denote by $\mathbb{Q}(r)$ the vector space $\mathbb{Q}$ with an action defined as $(g,q) \to \nu(g)^r q$. This action induces a Hodge structure on $\mathbb{Q}$ of weight $-2r$.

Proposition 2.3.12. *Lets (G,D) be a Shimura datum of Hodge type, i.e $(G,D) \hookrightarrow GS_p(V,\psi)$, where V is a vector space over $\mathbb{Q}$ of dimension $2n$. There exists non-zero multilinear maps*

$$t_i:\ V\times \overset{2r_i}{\cdots} \times V \to \mathbb{Q}(r_i)\ for i = 1,...,k$$

such that for any field extension $k/\mathbb{Q}$

$$G(k) = \{g \in GL_k(V)\ s.t\ t_i(gv_1,...,gv_{2r_i}) = \nu(g)^{r_i} t_i(v_1,...,v_{2r_i})\}$$

for all $v_j \in V(k)$ with $i = 1,...,k$.

Using the definition of $\mathbb{Q}(r_i)$, these maps are maps which $G(k)$ fixes. This proof can be found in [6, p. 77], and uses the Chevalley's theorem to find maps fixed by G.

As we explained previously, using our inherited complex structure J on $V(\mathbb{R})$, we obtain a decomposition of $V(\mathbb{R}) = V^+ \oplus V^-$. The interpretation of this result using the language of Hodge structures is that $V(\mathbb{R}) = V^{-1,0} \oplus V^{0,-1}$, obtaining a Hodge structure of weight -1 on $V(\mathbb{R})$. We can transfer this Hodge structure to the product of V, obtaining

$$V(\mathbb{R}) \times \overset{r}{\ldots} \times V(\mathbb{R}) = V(\mathbb{R})^{-r,0} \oplus V(\mathbb{R})^{-r+1,-1} \oplus \ldots \oplus V(\mathbb{R})^{0,-r}$$

Then, maps $t_i:\ V \times \overset{2r_i}{\ldots} \times \mathbb{Q}(r_i)$ are morphisms of Hodge structures of weight $-2r_i$.

Lets $K \subset G(\mathbb{A}_f)$ be a compact open subset. Lets $M_K(G,D)$ be the set of triples $(A, \{s_i\}_{i=0,\ldots,k}, \eta N)$ where

- A is a complex abelian variety of dimension n.
- s_0 is an alternating form on $H_1(A,\mathbb{Z})$ such that s_0 or $-s_0$ is a polarization on A.
- $s_i \in H^{2r_i}(A,\mathbb{Q}) \simeq Hom(\wedge^{2r_i}\Lambda, \mathbb{Q})$ such that $V^{2r_i} \to \wedge^{2r_i} V \to \mathbb{Q}(r_i)$ is a morphism of Hodge structures for $i = 1, \ldots, k$.
- $\eta:\ V(\mathbb{A}_f) \xrightarrow{\simeq} V_f(A)$ such that $\eta_*(\psi) = as$ for some $a \in \mathbb{A}_f^*$ and $\eta_*(t_i) = s_i$, for $i = 1, \ldots, k$.

Where those triples satisfy that there exists an isomorphism $\alpha : H_1(A,\mathbb{Q}) \simeq V$ of vector spaces over $\mathbb{Q}$ such that $\alpha_*(\psi) = qs$ for some $q \in \mathbb{Q}^*$, $\alpha_*(t_i) = s_i$ for $i = 1, \ldots, k$, and $\alpha_*(J) \in D_{(V,\psi)}$. Here J is the induced complex structure on $H_1(A,\mathbb{R})$.
An isomorphism from one triple $(A, (s_i)_i, \eta K)$ to a second $(A', (s'_i)_i, \eta' K)$ is an isomorphism $A \to A'$ sending s_0 to a multiple of s'_0 by an element of $\mathbb{Q}^*$. Also it sends each s_i to each s'_i and η to η' modulo K.

Observation 2.3.13. *In the previous third point, we can observe that given a map $s:\ V^{2r} \to \mathbb{Q}(r)$, it is a morphism of Hodge structures if and only if $s((V^{2r})^{p,q}) = 0$ for all pairs $(p,q) \neq (-r,-r)$. This is because the Hodge decomposition of $\mathbb{Q}$ by the action of ν^{r_i} has only one factor, of type $(-r,-r)$.*

Theorem 2.3.14. *The Shimura variety $Sh_K(G,D)$ is the coarse moduli space over $\mathbb{C}$ which classifies triples in $M_K(G,D)$ up to isomorphism. In particular, we have a bijection between the following sets*

$$M_K(G,D)/\simeq \longleftrightarrow G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$$

The proof of this theorem can be found in [6, p. 77] and it exploits the relation between abelian varieties and Hodge structures. In this case, we also use other new structures to construct the moduli space, which are related to Hodge structures.

Using this definition, we will be able to define the last Shimura variety which classifies abelian varieties, *PEL type*. To construct this variety we will need to introduce some concepts about algebras. We also need to make assumptions, if the reader is interested in this topic, the notes of Milne [6, p. 79] could be a great reference.

Lets $(B,*)$ be a semisimple algebra over $\mathbb{Q}$ with $*$ positive involution, i.e $*:\ B \to B$ involution such that $Tr_{B\otimes_{\mathbb{Q}}\mathbb{R}/\mathbb{R}}(b^*b) > 0$ for all $b \in B \setminus \{0\}$. We denote by F the center of B and $F_0 = \{b \in F\ s.t\ b^* = b\}$.
Assume that for every embedding $\phi:\ F_0 \hookrightarrow \overline{\mathbb{Q}}$, $(B \otimes_{F_0} \overline{\mathbb{Q}}, *)$ is isomorphic to a product of algebras with involution of only one of the two following forms

$$(A) \qquad M_n(\overline{\mathbb{Q}}) \times M_n(\overline{\mathbb{Q}}) \quad (b_1, b_2) = (b_2^t, b_1^t)$$

$$(B) \qquad M_n(\overline{\mathbb{Q}}) \quad b^* = b^t$$

This classification is given by a theorem of [6, prop. 8.3]. Its proof uses theory of conmutative algebra, and Skolem-Noether theorem to express the equation of the involution.

Lets (V, ψ) be a $(B, *)-$module, i.e a vector space V over $\mathbb{Q}$ together with an action $B \subset End(V)$ and a non-degenerate alternating bilinear form

$$\psi : V \times V \to \mathbb{Q} \text{ such that } \psi(bu, v) = \psi(u, b^* v), \text{ with } u, v \in V \text{ and } b \in B$$

Lets $G \subset GL(V)$ be the algebraic group over $\mathbb{Q}$ such that, for every field extension $K/\mathbb{Q}$ it satisfies

$$G(k) = \{g \in Aut_B(V \otimes k) \ s.t \ \psi(gu, gv) = \mu\phi(u, v)\}$$

for all $u, v \in V \otimes k$ and some $\mu(g) \in k^*$. The proof of the following two propositions can be found in [6, prop. 8.3, prop. 8.12, prop. 8.13] and relies on deep background in the theory of simplectic modules.

Proposition 2.3.15. *The algebraic group G is reductive.*

Proposition 2.3.16. *There exists a unique $G(\mathbb{R})-$conjugacy class D of homomorphisms $h : \mathbb{S} \to G_{\mathbb{R}}$ such that each h induces a symplectic complex structure $J = h(i)$ on $V(\mathbb{R})$ such that ψ_J is positive or negative definite. This Shimura datum satisfies the first three axioms.*

The last proposition gives us tools to construct a Shimura variety associated to an algebra (via G). The corresponding varieties $Sh(G, D)$ are called Shimura varieties of *PEL type.*
Lets $\{b_1, ..., b_k\}$ be a set of generators of B as a $\mathbb{Q}-$algebra, we define

$$\begin{aligned} t_{b_i} : \ & V \times V \to \mathbb{Q} \\ & (u, v) \to \psi(u, bv) \end{aligned}$$

Then (G, D) is the Shimura datum of Hodge type associated to (V, ψ) with $\{t_{b_i}\}$ as maps given by 2.3.12.

Lets $K \subset G(\mathbb{A}_f)$ be a compact subset. Lets $M_K(G, D)$ be the set of quadruples $(A, i, s, \eta K)$ where

- A is a complex abelian variety.
- $i : B \hookrightarrow End(A) \otimes \mathbb{Q}$.
- s is an alternating form on $H_1(A, \mathbb{Z})$ such that s or $-s$ is a polarization on A.
- $\eta : V(\mathbb{A}_f) \xrightarrow{\simeq} V_f(A)$ such that $\eta_*(\psi) = as$ for some $a \in \mathbb{A}_f^*$

satisfying that: There exists a $B-$linear isomorphism $\alpha : H_1(A, \mathbb{Q}) \simeq V$ of vector spaces over $\mathbb{Q}$ such that $\alpha^*(\psi) = qs$ for some $q \in \mathbb{Q}^*$.

Theorem 2.3.17. *The Shimura variety $Sh_K(G, D)$ is the coarse moduli space over $\mathbb{C}$ which classifies quadruples of $M_K(G, D)$ up to isomorphism.*

Proof. We can see that we have a correspondence between elements $b \in B$, that are also endomorphisms of $\mathbb{Q}$ (by definition) and maps $\{t_{b_i}\}$. These maps are used in the moduli interpretation of Hodge type to obtain a morphism of Hodge structure. By our correspondence, we can express this condition as $B \hookrightarrow End(A) \otimes \mathbb{Q}$. ∎

2.4 Canonical models

With the help of Baily-Borel's theorem, we deduced that Shimura varieties are algebraic varieties, then they are defined by a set of polynomials. In order to study Shimura varieties in an arithmetic setting, a natural question would be *"What is the "natural" field of definition of those varieties?"*. The *reflex field* will give us the answer to our question. Also, in this section, we are going to define what is a canonical model of a Shimura variety, the standard algebraic-geometric definition of Shimura varieties. In this section we will define *special points*, we can understand these points as the generators of each Shimura variety. We will study some properties about these points to prove the uniqueness of the canonical model. From a number theory point of view, these points will encode the arithmetic information about our problem, an example of this phenomena can be seen at sections 5 and 6 of chapter 3.

For G reductive algebraic group over $\mathbb{Q}$ and k subfield of $\mathbb{C}$, we define $\mathfrak{C}(k)$ as the set of $G(k)-$conjugacy classes of cocharacters of G_k defined over k

$$\mathfrak{C}(k) = G(k) \setminus Hom(\mathbb{G}_m, G_k)$$

We can see that this definition is compatible with the field homomorphisms, since given $k \to k'$ an homomorphism, this induces a map $\mathfrak{C}(k) \to \mathfrak{C}(k')$. Also, the group $Aut(\mathbb{C}/k)$ acts on $\mathfrak{C}(k)$. Given $\sigma \in Aut(\mathbb{C}, k)$ and $a \in \mathfrak{C}(k)$, $\sigma(a(b)) = a(\sigma(b))$.

Lemma 2.4.1. *Lets T be a split maximal torus in G_k, $W = N_G(\overline{\mathbb{Q}}))/Z_G(T(\overline{\mathbb{Q}}))$, then there exists a bijection between*

$$W \setminus Hom(\mathbb{G}_m, T_k) \longleftrightarrow G(k) \setminus Hom(\mathbb{G}_m, G_k)$$

The proof of the previous lemma can be found in [6, lem. 12.1], and it relies with theory about algebraic groups.
Given $x \in D$, and $h_x : \mathbb{S} \to G_{\mathbb{R}}$ its associated map, we can define a cocharacter as

$$\begin{aligned} \mu_x : \mathbb{C}^* \to \mathbb{S}(\mathbb{C}) = \mathbb{C} \times \mathbb{C} \to G_{\mathbb{C}} \\ z \to (z, 1) \longrightarrow h_{\mathbb{C}}(z, 1) \end{aligned}$$

We deduce that for any other point $x \in D$, the associated morphism is conjugated to h_x, and then $\mu_x \in \mathfrak{C}(\mathbb{Q})$ is independet of the choice of x. We denote this cocharacter as $c_D \in \mathfrak{C}(\mathbb{Q})$. Using the previous lemma, we can see that c_D is defined over a number field. This is deduced by the correspondence

$$\left\{ \begin{matrix} W-conjugacy\ classes \\ in\ Hom(\mathbb{G}_m, T_{\overline{\mathbb{Q}}}) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} W-conjugacy\ classes \\ in\ Hom(\mathbb{G}_m, T_{\mathbb{C}}) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} G(\mathbb{C})\ conjugacy\ classes \\ in\ Hom(\mathbb{G}_m, G_{\mathbb{C}}) \end{matrix} \right\}$$

due to the fact that T is split.

Definition 2.4.2. The *reflex field* $E(G, D)$ of the Shimura datum (G, D) is the field of definition of c_D as an element of $\mathfrak{C}(\overline{\mathbb{Q}})$, that is, the field fixed by $\{\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}) :\ c_D^{\sigma} \cong c_D \in \mathfrak{C}(\overline{\mathbb{Q}})\}$.

Examples 2.4.3. *1. Lets (E, Φ) be a CM-type, that is, E be an imaginary quadratic extension of a totally real number field and $\Phi = \{\phi_1, ..., \phi_g\} \subset Hom(E, \mathbb{C})$ such that $Hom(E, \mathbb{C}) = \Phi \cup \overline{\Phi}$ (a full set of representatives of embeddings $E \hookrightarrow \mathbb{C}$ up to complex conjugation).*
Let $T = Res_{E/\mathbb{Q}}\mathbb{G}_m$. Due to the fact that for any choice of $g-$inequivalent embeddings $\{\phi_1, ..., \phi_g\}$ we can define an isomorphism such that

$$\begin{aligned} E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathbb{C} \times \overset{g}{\cdots} \times \mathbb{C} \\ a \otimes r \to (\phi_1(a)r, ..., \phi_g(a)r) \end{aligned}$$

Then we have that $T(\mathbb{R}) = (E \otimes_{\mathbb{Q}} \mathbb{R})^* \simeq \mathbb{C}^*_{\phi_1} \times ... \times \mathbb{C}^*_{\phi_g}$. We define the homomorphism $h_\Phi :\ \mathbb{S} \to T_{\mathbb{R}}$ as

$$\begin{aligned} h_\Phi :\ \mathbb{S}(\mathbb{R}) = \mathbb{C}^* \to T(\mathbb{R}) = (\mathbb{C}^*)^g \\ z \to (z, ..., z) \end{aligned}$$

The map $h_{\Phi,\mathbb{C}}$ will be the map which makes the following diagram a conmutative diagram

$$\begin{array}{ccc} \mathbb{S}(\mathbb{R}) & \xrightarrow{h} & T(\mathbb{R}) \\ \downarrow & & \downarrow \\ \mathbb{S}(\mathbb{C}) & \xrightarrow{h_{\mathbb{C}}} & T(\mathbb{C}) \end{array}$$

To find its expression, we have to find maps $\mathbb{S}(\mathbb{R}) \to \mathbb{S}(\mathbb{C})$ and $T(\mathbb{R}) \to T(\mathbb{C})$. We can define those maps as

$$\mathbb{S}(\mathbb{R}) = (\mathbb{C})^* \to \mathbb{S}(\mathbb{C}) = (\mathbb{C} \times \mathbb{C})^*$$
$$z \longrightarrow (z, \overline{z})$$

$$T(\mathbb{R}) = (\mathbb{C}^*)^g \to T(\mathbb{C}) = (\mathbb{C}^*)^{2g}$$
$$(z_1, ..., z_g) \to (z_1, ..., z_g, \overline{z_1}, ..., \overline{z_g})$$

using embeddings $E \hookrightarrow \mathbb{C}$ as before. Now, we define maps which makes our diagram conmutative.

$$(h_\Phi)_{\mathbb{C}} : \ \mathbb{C}^* \times \mathbb{C}^* \to (\mathbb{C}^*)^g \times (\mathbb{C}^*)^g$$
$$(z_1, z_2) \to (z_1, ..., z_1, z_2, ..., z_2)$$

Using the previous reasoning, we obtain the cocharacter

$$\mu_{\Phi,\mathbb{C}} : \ \mathbb{C}^* \to (\mathbb{C}^*)^g \times (\mathbb{C}^*)^g$$
$$z \to (z, ..., z, 1, ..., 1)$$

As the map h_Φ is defined in each coordinate by the embeddings $E \hookrightarrow \mathbb{C}$, the reflex field, $E(T, h_\Phi)$ by definition is the fixed field of $\{\sigma \in Aut(\overline{\mathbb{Q}}/\mathbb{Q}) : \ \Phi^\sigma = \Phi\}$. This is because our cocharacer is based on the position of the coordinates, given by our embeddings. This field is called the reflex field of the CM type (E, Φ), and has the following characterizations:

- *$\widetilde{E}$ is the fixed field of $\{\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}) : \ \Phi^\sigma = \Phi\}$.*
- *$\widetilde{E} = \mathbb{Q}(\sum_{\phi\in\Phi} \phi(a) : \ a \in E)$.*
- *It is the smallest subfield of $\overline{\mathbb{Q}}$ for which there exists an $\widetilde{E}-$vector space V together with a morphism $E \hookrightarrow End_{\widetilde{E}}(V)$ for which $Tr(a) = \sum_{\phi\in\Phi} \phi(a)$ for all $a \in E$.*

2. *If we have T a torus defined over $\mathbb{Q}$, and x a point, we can define a Shimura variety as in last section*
$$Sh_K(T, x) = G(\mathbb{Q}) \setminus G(\mathbb{A}_f)/K$$
Lets $h : \ \mathbb{S} \to T_{\mathbb{R}}$ be an homomorphism. Then $\mu_h : \ G_{m,\mathbb{C}} \to T_{\mathbb{C}}$ is defined over $\overline{\mathbb{Q}}$. Its reflex field $E = E(T, \{h\})$ is the fixed field of the subgroup $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ which fixes μ_h.

3. *Lets $i : \ (G, D) \hookrightarrow (G', D')$ be an inclusion of Shimura data. There is a natural morphism of Shimura varieties $Sh(G, D) \hookrightarrow Sh(G', D')$ which is a closed inmersion, we can show that $E(G', D') \subseteq E(G, D)$. This is because if we have an inmersion of D, then we will have an inmersion of maps h. If we have that $D \subset D'$ and $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes μ'_x which comes from $h' \in D'$, then σ will fix every μ_x which comes from $h \in D$.*

4. *Also, we can compute the reflex field for the Siegel modular variety. Lets (V, ψ) be a symplectic vector space over $\mathbb{Q}$ of dimension $2n$. Lets $G = GSp(V, \psi)$ and $D = D^+ \cup D^-$ be the set of positive or negative symplectic complex strutures J on $V(\mathbb{R})$. We can obtain a symplectic basis of V such that $V =< e_1, .., e_n, \widetilde{e_1}, ..., \widetilde{e_n} >$. This basis gives a division of V as*

$$V = W \oplus \widetilde{W}$$

where each component is generated by a part of the symplectic basis. We can define $J \in End(V)$ such that $J(e_i) = \widetilde{e_i}$ and $J(\widetilde{e}_i) = -e_i$. The map of this Shimura variety which we defined is

$$h_J(a+bi) = a + bJ$$

Then, as we did before, we need the map $h_{J,\mathbb{C}}$ which closes the diagram with the transition map $\mathbb{S}(\mathbb{R}) \to \mathbb{S}(\mathbb{C})$ as before. We can define this map as

$$h_{J,\mathbb{C}}(z_1, z_2) = (a_1 + b_1 J, a_2 - b_2 J) \in End(V(\mathbb{C}))$$

We can express each endomorphism of our vector space as a matrix, making easier computations. Then we define the cocharacter

$$\begin{aligned} c_{h_J}:\ \mathbb{C}^* \to G_{\mathbb{C}} &\xrightarrow{id} End(V^+ \oplus V^-) \\ z \to h_{J,\mathbb{C}}(z,1) &\to \begin{pmatrix} z & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Definition 2.4.4. Lets (G, D) be a Shimura datum, a point $x \in D$ is a *special point* if there exists a torus defined over $\mathbb{Q}$, $T \subset G$ such that $h_x(\mathbb{C}^*) \subset T(\mathbb{R})$.
We name a pair (T, x) (with T and x as before) a *special pair.*

Observation 2.4.5. *Given a special pair (T, x), we have a inclusion of Shimura data $(T, x) \xrightarrow{i} (G, D)$. Since $h_x(\mathbb{C}^*) \subset T(\mathbb{R})$, and $T(\mathbb{R})$ is a conmutative group, we have that $th_xt^{-1} = h_x$ for any $t \in T(\mathbb{R})$, and then $T(\mathbb{R})$ fixes the point $x \in D$. Conversely, if $T \subset G$ is a maximal torus and $x \in D$ is a point fixed by a set of elements of $T(\mathbb{R})$, then $h(\mathbb{C}^*) \subset \{g \in G(\mathbb{R}) :\ gt = tg\ \forall t \in T(\mathbb{R})\} = T(\mathbb{R})$ because T it is its own centralizer in G.*

Example 2.4.6. *1. Lets $G = GL_2$ and lets $\mathcal{H}_1 = \mathbb{C} \setminus \mathbb{R}$. Then we have the classical action defined as*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

Lets $z \in \mathbb{C} \setminus \mathbb{R}$ such that generates a quadratic extension E of $\mathbb{Q}$. We have embeddings $\mathbb{G}_m \xrightarrow{a \to aId_2} GL_2$ and $T = Res_{E/\mathbb{Q}}\mathbb{G}_m \to GL_2$ (the latter, defined by the inclusion $E \hookrightarrow GL_2(\mathbb{R})$ when we choose the basis $\{1, z\}$ of E). Now we can observe that using the fact that $T(\mathbb{R}) = \mathbb{C}^*$, we have an inclusion $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^* \to T(\mathbb{R}) = \mathbb{C}^*$. This map provides us special pairs. To show what points fixes each special pair, we use the structure of $E \otimes \mathbb{C}$, that is a $\mathbb{C}-$vector space with basis $\{1 \otimes 1, 1 \otimes (-z)\}$. With this basis, we can embed this vector space into GL_2. The kernel of the map

$$\begin{aligned} E \otimes \mathbb{C} &\to \mathbb{C} \\ e \otimes z &\to ez \end{aligned}$$

is the space spanned by $\{z \otimes 1 + 1 \otimes (-z)\}$, that, with respect to our basis is $(z, 1)$, which represents the point z which we have chosen. Since the map is $E \otimes \mathbb{R}-$linear, we have that $(E \otimes \mathbb{R})^*$ fixes z.

Lets (T, x) be a special pair of a Shimura datum (G, D). Lets $E(x) = E(T, x)$ its reflex field, i.e, the field of definition of μ_x. It is a finite extension of $E = E(G, D)$. Lets $r(T, \mu_x)(P) : Res_{E/\mathbb{Q}}\mathbb{G}_m \to T$ such that

$$r(T, \mu_x)(P) = \sum_{\sigma\colon E \to \overline{\mathbb{Q}}} \mu_x(P)^\sigma$$

Using this homomorphism, we can define a map, which we will use to define what is a canonical model

$$r_x : \mathbb{A}^*_{E(x)} \xrightarrow{r(T,\mu_x)} T(\mathbb{A}_{\mathbb{Q}}) \xrightarrow{projection} T(\mathbb{A}_{\mathbb{Q},f})$$

We are going to work with adéles, then, it will be necessary one of the most important theorems about class field theory, the *Artin reciprocity map*. Its proof uses tools from class field theory and can be found at [13, p. 113].

Theorem 2.4.7 (Artin reciprocity law). *Lets E be a number field, and lets E^{ab} be the maximal abelian extension of E inside a fixed algebraic closure E. We have the following continuous surjective homomorphism*

$$rec_E : \mathbb{A}_E^* \twoheadrightarrow Gal(E^{ab}/E)$$

This map has the property that for any finite abelian extension E'/E of E, we have a conmutative diagram as follows

$$\begin{array}{ccc} E^* \setminus \mathbb{A}_E^* & \xrightarrow{rec_E} & Gal(E^{ab}/E) \\ \downarrow & & \downarrow \\ E^* \setminus \mathbb{A}_E^*/Nm_{E'/E}(\mathbb{A}_{E'}^*) & \xrightarrow{rec_{E'/E}} & Gal(E'/E) \end{array}$$

The identity component of $\mathbb{A}_E^*$ lies in the kernel of rec_E. Then, if E is totally imaginary, rec_E factors through $\mathbb{A}_{E,f}^*$.

Definition 2.4.8. Lets k be a subfield of a field Ω, lets V be a variety over Ω. A *model* of V over k is a variety V_0 together with an isomorphism

$$\phi : V_{0,\Omega} \to V$$

Observation 2.4.9. *We often omit the map ϕ and we regard a model as a variety V_0 defined over k such that $V_{0,\Omega} = V$. This is because if we have Λ field such that $\Omega \subset \Lambda$, then $V_{0,\Omega}(\Lambda) = V_0(\Lambda) \otimes_\Lambda \Omega = V(\Lambda)$. Intuitively, a model over a field is that we can define this variety with equations over this field.*

Example 2.4.10. *If we have the variety $(x+i)(x-i) = 0$, we have that a priori it is defined over $\mathbb{C}$, but we can express the same variety over $\mathbb{R}$ using $x^2 + 1 = 0$ which has the same set of points as the first variety over any field.*

Observation 2.4.11. *If we have an affine variety V over $\mathbb{C}$, in general it will not have model over a given subfield k of $\mathbb{C}$. This variety has a model over k if the ideal $I(V)$ is generated by polynomials in $k[X_1, ..., X_n]$, because then $I' = I(V) \cap k[X_1, ..., X_n]$ is a radical ideal and by Nullstellensatz it will generate a variety.*

Proposition 2.4.12. *Lets k be a subfield of an algebraically closed field Ω of characteristic 0. Let V and W be varieties over k. Then every regular map $V_\Omega \to W_\Omega$ commuting with the actions of $Aut(\Omega/k)$ on $V(\Omega)$ and $W(\Omega)$ arises from an unique regular map $V \to W$*

Proof. Its proof can be found at [12, prop. 16.9] and uses Zorn's Lemma. ∎

We write $[x, a]_K$ for an element of

$$Sh_K(G, D) = G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$$

represented by $(x, a) \in D \times G(\mathbb{A}_f)$.

Definition 2.4.13. Lets (G, D) be a Shimura datum, and lets K be a compact open subgroup of $G(\mathbb{A}_f)$. A *canonical model* over $E(G, D)$ is an algebraic model $M_K = M_K(G, D)$ with

$$M_K(G, D) \simeq Sh_K(G, D)$$

such that for any special pair $(T, x) \subset (G, D)$, and any $a \in G(\mathbb{A}_f)$:

- $(x, a) \in M_K(E(x)^{ab})$.

- $(x,a)^{rec(s)} = (x, r_x(s^{-1})a)$ for any $s \in \mathbb{A}^*_{E(x)}$.

The last point can be rewritten as $\sigma(x,a) = (x, r_x(s)a)$ with $art_{E(x)}s = \sigma$.

Observation 2.4.14. *This definition says that each Shimura variety is defined by its special points.*

Definition 2.4.15. A *model* of $Sh(G,D)$ over a subfield k of $\mathbb{C}$ is an inverse system $M(G,D) = (M_K(G,D))_K$ of varieties over k with the right action of $G(\mathbb{A}_f)$ such that $M(G,D)_{\mathbb{C}} = Sh(G,D)$.

A model $M(G,D)$ of $Sh(G,D)$ over $E(G,D)$ is *canonical* if each $M_K(G,D)$ is canonical.

Examples 2.4.16. 1. *Lets T be a torus over $\mathbb{Q}$ and $K \subset T(\mathbb{A}_f)$. We can construct a Shimura variety as in the example of the previous subsection.*

$$Sh_K(T,x) = T(\mathbb{Q}) \setminus T(\mathbb{A}_f)/K$$

This quotient is finite by Borel's theorem (2.1.5). Then, a model over $E = E(x)$ of a finite set of points, is the action of $Gal(\overline{E}/E)$ on it. We can use Artin reciprocity map to obtain

$$Gal(\overline{E}/E) \to Gal(E^{ab}/E) \twoheadrightarrow Gal(H_K/E) \xrightarrow{\simeq \text{ by } rec_{H_K/E}} E^* \setminus \mathbb{A}^*_E/K$$

Where H_K is the field obtained by applying the artin reciprocity map. Then we can define the action as in the definition, $a^s = r_x(s^{-1})a$ with $a \in T(\mathbb{A}_f)$ and $s \in \mathbb{A}^*_{E(x)}$. It is a continuous action, and it is well defined by the above chain.

2. *Lets (E,Φ) a CM-type as in previous examples, and $K \subset T(\mathbb{A}_f)$ open compact subgroup. Lets $T = Res_{E/\mathbb{Q}}\mathbb{G}_m$, and as we proved, $E(h_\Phi) = \widetilde{E}$. We can define a Shimura variety as*

$$Sh_K(T,h_\Phi) = E^* \setminus \mathbb{A}^*_{E,f}/K$$

Using the Artin reciprocity map, we can transfer elements of the Shimura variety to the Galois group

$$\widetilde{E} \setminus \mathbb{A}_{\widetilde{E},f}/K \xrightarrow{\simeq \text{ by } rec} Gal(H_K/\widetilde{E})$$

Then we define the action of the Galois group as in the definition

$$a^s = r_{h_\Phi}(s^{-1})a = \prod_{\sigma:\widetilde{E}\hookrightarrow\overline{Q}} \mu_\Phi(s^{-1})^\sigma a = det_{\mathbb{A}_{E,f}}(s^{-1})a$$

If we set E as an imaginary quadratic extension and $\Phi = \{\phi\}$ the inclusion, we have a $CM-$type. Then by the second characterization of its reflex field $\widetilde{E} = E$. Then we can define the map μ_Φ as

$$\mu_\Phi : \widetilde{E}^* \to T(\widetilde{E}) = (E \otimes_{\mathbb{Q}} \widetilde{E})^* = (\widetilde{E} \times \widetilde{E})^*$$

As usual, we have defined the map μ over $\mathbb{C}$. In this case, we have used the fact that $\widetilde{E} \subset \mathbb{C}$. The action of $Gal(\widetilde{E}/\mathbb{Q})$ on $T(\widetilde{E})$ is given by $(z_1,z_2)^\sigma = (z_2^\sigma, z_1^\sigma)$. Then, we have the embedding

$$\begin{aligned} T(\mathbb{Q}) = E^* &\xrightarrow{i} T(\widetilde{E}) \\ s &\to (s, s^\sigma) \end{aligned}$$

Then to compute $\prod_{\sigma:\widetilde{E}\to\overline{\mathbb{Q}}} \mu_\Phi(s)^\sigma$, we have two embeddings $\sigma : \widetilde{E} \hookrightarrow \overline{\mathbb{Q}}$; the identity and the conjugation. Then, applying the formula which we defined for the Galois action we have that $\prod_{\sigma:\widetilde{E}\to\overline{\mathbb{Q}}} \mu_\Phi(s)^\sigma = (s,1)(1,\overline{s}) = (s,\overline{s}) = i(s)$. Last equality is due to Shimura-Taniyama theorem.

Last example is very interesting, it is a moduli space. Lets (T, h_Φ) be the previous $CM-$Shimura datum. $Sh_K(T, h_\phi)$ is a finite set of points, that we can see a Shimura variety of PEL type associated to E as a conmutative algebra.

Specifically we say that $Sh_K(T, h_\Phi)$ classifies up to isomorphism classes of triples $(A, i, \eta K)$ with (A, i) an abelian variety over $\mathbb{C}$ of $CM-$type (E, Φ) and η a $E \times \mathbb{A}_f-$linear isomorphism

$$V(\mathbb{A}_f) \to V_f(A)$$

In this moduli space we define an isomorphism $M_K = (A, i, \eta K) \to M'_K = (A', i', \eta' K)$ as a linear $E-$isomorphism $A \to A'$ in the category of abelian varieties which sends ηK to $\eta' K$.

Also, we can find the canonical model of this variety. Lets $\sigma \in Gal(\overline{\mathbb{Q}}/E^*)$. This map acts on the triples $(A, i, \eta) \in Sh_K(T, h_\Phi)$ as follows

$$\sigma(A, i, \eta K) = (\sigma A, i^\sigma, \eta^\sigma K)$$

where η^σ is the following composition

$$V(\mathbb{A}_f) \xrightarrow{\eta} V_f(A) \xrightarrow{\sigma} V_f(\sigma A)$$

Using that σ fixes E^*, then the pair $(\sigma A, \sigma i)$ is again a $CM-$type (E, Φ). Since we have defined an action on this moduli problem, we can define the action in our Shimura variety. We define the action on the Shimura variety as in the definition 2.4.13.

$$\sigma(g) = (r_{h_\Phi}(s)g) \quad \textit{with} \quad art_{E^*}(s) = \sigma|_{E^*}$$

Then this defines a model of $Sh_K(T, h_\Phi)$ over E^*.

Proposition 2.4.17. *The map*

$$\begin{aligned} M_K &\to Sh_K(T, h_\phi) \\ (A, i, \eta) &\to [a \circ \eta]_K \end{aligned}$$

conmutes with the action of $Gal(\overline{\mathbb{Q}}, E^*)$*. With a a certain map* $a: H_1(A, \mathbb{Q}) \to V$.

The proof of this proposition can be found at [6, p. 116] and it relies on deep background in the theory of abelian varieties.
This proposition proves that the previous model is a canonical model.

Proposition 2.4.18. *Lets* (G, D) *be a Shimura datum. There exists a special point in* X*.*

Proof. Let $\mathfrak{g}$ be a Lie algebra over k algebraically closed field of characteristic zero. We can define Cartan subalgebras as subalgebras nilpotents and equal to their own normalizer. If $\mathfrak{g}$ is the Lie algebra of a semisimple algebraic group G over k, then we can characterize Cartan subalgebras as Lie algebras of maximal tori in G.
Lets $P_x(T) = det(T - ad(x))$ be the characteristic polynomial of an element $x \in \mathfrak{g}$. We can express this polynomial as

$$P_x(T) = T^n + a_{n-1}(x)T^{n-1} + \cdots + a_r(x)T^r$$

where a_i defines regular functions on $\mathfrak{g}$ and $a_r \neq 0$. We say that $x \in \mathfrak{g}$ is regular if $a_r(x) \neq 0$. If we use the Zariski topology for $\mathfrak{g}$, the set of regular points is dense. This points are related to Cartan subalgebras because Cartan subalgebras are exactly the centralizers of regular elements of $\mathfrak{g}$, also, any two are conjugated by inner automorphism.

Lets (G, D) be a Shimura datum. Lets $x \in D$, and lets T be a maximal torus containing $h_x(\mathbb{C})$. Then, using the second characterization of the Cartan subalgebra, we have that, as G is a semisimple algebraic group, $\mathfrak{t} = Lie(T)$ is a Cartan subalgebra, and then it is the centralizer in

$G_{\mathbb{R}}$ of a regular point $\lambda \in Lie(G_{\mathbb{R}})$. The set of regular points is dense, this means that we can find an element λ_0 in some neighborhood which contains λ, such that its centralizer $\mathfrak{t}_0$ has associated a Lie group T such that it is a maximal torus in G.
We have done a correspondence between Lie groups and Lie algebras, but this theorem gives us an unique correspondence if the Lie groups and algebras were connected. This is not our case, and then if we had selected a random regular point, maybe the maximal tori associated to each point would not be conjugated of each other. If we choose λ_0 enought close to λ, this point will be in the same connected component, and then its tori will be conjugated by inner automorphism (We can translate the fact of being conjugated as Lie algebras to being conjugated as Lie group by the previous correspondence, then, from now on we are going to write the theory in terms of Lie groups).

Let's denote by T_0 the maximal torus associated to λ_0, then, by the previous reasoning, we have that

$$T_{0,\mathbb{R}} = gTg^{-1} \quad for\ some\ g \in G(\mathbb{R})$$

now we can define

$$h_{gx}(\mathbb{S}) = ghg^{-1}(\mathbb{S}) \subset T_{0,\mathbb{R}}$$

obtaining that gx is a special point. ∎

Lemma 2.4.19. *For every finite extension L of $E(G, D)$ in $\mathbb{C}$, there exists a special point x_0 such that $E(x_0)$ is linearly disjoint from L.*

Observation 2.4.20. *In the previous lemma, the expression $E(x_0)$ with $x_0 \in X$ means that, as D is an hermitian symmetric domain, then it is isometric to some open set $D' \subset \mathbb{C}^n$ with the Bergam's metric (the next paragraph to (1.1)). Then, if we name this isomorphism by i, thus $E(x_0) := E(i(x_0))$.*

We can find the proof of the previous theorem at [5, prop. 5.1], which uses the Hilbert irreducibility theorem.

Lemma 2.4.21. *For any $x \in D$, $\{[x, a]_K\ s.t\ a \in G(\mathbb{A}_f)\}$ is dense in $Sh_K(G, D)$ with the Zariski topology.*

Proof. We can write

$$Sh_K(G, D)(\mathbb{C}) = G(\mathbb{Q}) \setminus D \times G(\mathbb{A}_f)/K$$

then, as the definition of D is the $G(\mathbb{R})-$conjugacy class of some element $x \in D$, then if we select $x \in D$, using real approximation 2.1.9, since $G(\mathbb{Q})x$ is dense in $G(\mathbb{R})x$, then $G(\mathbb{Q})$ is dense in the $G(\mathbb{R})-$conjugacy class of x, that is D (with the complex topology). We deduce that $G(\mathbb{Q}) \times G(\mathbb{A}_f)$ is trivially dense in $D \times G(\mathbb{A}_f)$, and then its image in $Sh_K(G, X)(\mathbb{C})$ is dense for the complex topology, and then for the Zariski topology.

The image of $G(\mathbb{Q})x \times G(\mathbb{A}_f)$ in $Sh_K(G, D)$ equals

$$\{[x, a]_K\ s.t\ a \in G(\mathbb{A}_f)\}$$

This is because $[gx, b]_K = [x, g^{-1}b]_K$ for $g \in G(\mathbb{Q})$ and $b \in G(\mathbb{A}_f)$. ∎

Lets $g \in G(\mathbb{A}_f)$ and let K, K' be compact open subgroups such that $g^{-1}Kg \in K'$. Lets (G, D) be a Shimura datum, we define the following map between varieties

$$\begin{aligned} \mathcal{T}(g):\ Sh_k(\mathbb{C}) &\to Sh_{K'}(\mathbb{C}) \\ [x, a]_K &\to [x, ag]_{K'} \end{aligned}$$

This map is well defined, and it is a morphism of algebraic varieties over $\mathbb{C}$ by [6, thm. 3.14].

Theorem 2.4.22. *If $Sh_K(G, D)$ and $Sh_{K'}(G, D)$ have canonical models over $E(G, X)$, then $\mathcal{T}$ is defined over $E(G, X)$.*

Proof. We can see those Shimura varieties as varieties defined over $\mathbb{C}$, then, if we apply 2.4.12 with $\Omega = \mathbb{C}$, $k = E(G, D)$, we can reduce this problem to show that the diagram is conmutative for $\sigma \in Aut(\mathbb{C}/E)$. This condition can be rewritten as $\sigma(\mathcal{T}(g)) = \mathcal{T}(g)$ for all $\sigma \in Aut(\mathbb{C}/E)$.

Lets x_0 be an special point of D. Then this point defines an element of $\mathfrak{C}(k)$ defined in $E(x_0)$. Therefore $E(G, D) \subset E(x_0)$ trivially because x_0 is fixed by the automorphism which fixes $E(G, D)$. First, we are going to show that $\sigma(\mathcal{T}(g)) = \mathcal{T}(g)$ for σ which fixes $E(x_0)$. Using that we have canonical models, we can choose $s \in \mathbb{A}^*_{E_0}$ such that $art(s) = \sigma|E(x_0)^{ab}$. Then for $a \in G(\mathbb{A}_f)$,

$$\begin{array}{ccc} [x_0, a]_K & \xrightarrow{\mathcal{T}(g)} & [x_0, ag]_{K'} \\ \downarrow & & \downarrow \\ [x_0, r_{x_0}(s)a]_K & \xrightarrow{\mathcal{T}(g)} & [x_0, r_{x_0}(s)ag]_{K'} \end{array}$$

This diagram is conmutative, with the down arrows given by applying σ. We observe that $\sigma(\mathcal{T}(g)) = \mathcal{T}$ agree on $\{[x_0, a]\ s.t\ a \in G(\mathbb{A}_f)\}$. Then, since this set is dense in Sh_K by lemma 2.4.21, we have proved that $\sigma(\mathcal{T}(g)) = \mathcal{T}(g)$ for all σ which fix the reflex field of any special point. Using the lemma 2.4.19, we conclude that these σ generate $Aut(\mathbb{C}/E(G, D))$. ∎

Theorem 2.4.23. 1. *If there exists a canonical model of $Sh_K(G, D)$, then it is unique up to isomorphism.*

2. *If for all compact open subgroup $K \subset G(\mathbb{A}_f)$ the Shimura variety $Sh_K(G, D)$ has a canonical model. We can assert that $Sh(G, X)$ also has an unique canonical model up to isomorphism.*

Proof. 1. Take $K = K'$ and $g = 1$ in theorem 2.4.22.

2. It follows trivially from 2.4.22.

∎

A very important part in the theory of canonical model is that we always can find a canonical model for a Shimura variety. This is a very important result because when we have a Shimura variety, we know that this Shimura variety is defined by a set of equations which gives to this variety a structure which has well behaviour with respect the automorphisms and it is defined over a certain number field. This theorem gives us an arithmetic interpretation about Shimura varieties.

Theorem 2.4.24. *Given a Shimura variety, there exists a canonical model for this variety*

The outline of its proof can be found at [6, p. 125]. This proof is very deep and uses complicated theory about algebraic geometry.

2.5 Quaternionic Shimura varieties

The main result of this dissertation is to prove the Gross-Zagier formulae. This result, gives the special value of a family of $L-$functions in terms of special points of a Shimura variety. In this subsection, we are going to define this type of Shimura variety, the *quaternionic Shimura variety*. We are going to study this variety, applying all the theory that we have used until now.

First, we are going to see a construction given a indefinite quaternion algebra B. This construction gives us a great family of quaternionic Shimura varieties (not all). This method is interesting because we can see explicitly how they work. Later we will describe the general case for quaternion algebras, using tools and the theory stated before. As we can observe, we can divide into two families those quaternionic Shimura curves, *definites* and *indefinites*. These names come from the quaternion algebra which defines them. The election of the quaternion algebra makes a clear division into those varieties respect to their behaviour. Definite quaternionic Shimura varieties are a finite set of points, and therefore they have a simpler structure. In contrast, indefinite quaternionic Shimura varieties can be seen as the higher dimensional version of a modular curve. This enormous change is due to the fact that being definite or not will define how the algebraic group acts on the Hermitian symmetric domain.

Lets B be an indefinite quaternion algebra. The quaternion algebra B splits in some places, this means that

$$B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})^r \times \mathbb{H}^{n-r}$$

with n the number of real places of F and $r > 0$. This result can be understanded as in the case of $CM-$type. In ths case we had a totally real field, with some embeddings which gives us the way to express $E \otimes_{\mathbb{Q}} \mathbb{R}$. Lets

$$i_\infty : \ B \hookrightarrow M_2(\mathbb{R})^r$$

the embedding given by the split places of B. This map allows us to see elements of the quaternion algebra as matrices, and then associate some properties via i_∞. We define the following group

$$B_+^* = \{\gamma \in B^* \ s.t \ det \ \gamma_i = (nrd \ \gamma)_i > 0 \ for \ i = 1, ..., r\}$$

Where γ_i means the $i-$th coordinate of $i_\infty \gamma$. Then we can associate an action of B^* on $\mathcal{H}^r$, the Moebius transformation in each coordinate.
Lets $\mathcal{O}_1$ be a maximal order in B and $\mathfrak{N} \subseteq \mathbb{Z}_F$ a coprime ideal with the discriminant of B, $\mathfrak{D}$. As with the quaternion algebra, we can do tensor products by complections of $\mathbb{Z}_F$, giving embeddings

$$i_{\mathfrak{N}} : \ \mathcal{O}_1 \hookrightarrow O_1 \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \simeq M_2(\mathbb{Z}_{F,\mathfrak{N}})$$

where $\mathbb{Z}_{F,\mathfrak{N}}$ is the complection respect $\mathfrak{N}$ of the ring of integers of F. Using this map we define

$$\mathcal{O}_1(\mathfrak{N}) = \{x \in \mathcal{O}_1 \ s.t \ i_{\mathfrak{N}}(x) \ \textit{is upper triangular modulo} \ \mathfrak{N}\}$$

We will see that $\mathfrak{N}$ will determine the level structure of the Shimura variety. We are going to denote by $\mathcal{O}$ to $\mathcal{O}(\mathfrak{N})$, which in fact, is an Eichler order (definition in [1]). We define

$$\mathcal{O}_+^* = \mathcal{O}^* \cap B_+^*$$

Assuming that F has strict class number 1, we have that

$$\mathcal{O}_+^* = \mathbb{Z}_F^* \mathcal{O}_{id}^*$$

with $\mathcal{O}_{id} = \{\gamma \in \mathcal{O} \ s.t \ nrd(\gamma) = 1\}$. Then we define

$$\Gamma = \Gamma_0^B(\mathfrak{N}) = i_\infty(\mathcal{O}_+^*) \subseteq GL_2^+(\mathbb{R})^r$$

If we compare Shimura varieties with modular curves, this will be the equivalent object to the congruence subgroup. We define a Shimura variety as

$$\Gamma_0^B(\mathfrak{N}) \setminus \mathcal{H}^r$$

With this construction we can find indefinite Shimura varieties controlling each computation. Despite this is an easy construction, we can not create definite varieties in this way, this is due to the fact that we could not obtain this type of actions.

In the general case, lets B be a quaternion algebra over F totally real field. We are going to denote by Σ_∞ the set of infinity places of F. Also, if Σ_B is the set of places of F where B is ramified, we define $\Sigma_{B,\infty} = \Sigma_B \cap \Sigma_\infty$. Then, each place gives us an isomorphism

$$B \otimes_{F,\sigma} \mathbb{R} \simeq M_2(\mathbb{R}) \ for \ \sigma \in \Sigma_\infty \setminus \Sigma_B \tag{2.2}$$

$$B \otimes_{F,\sigma} \mathbb{R} \simeq \mathbb{H} \; for \; \sigma \in \Sigma_{B,\infty} \tag{2.3}$$

Lets $G_B = Res_{F/\mathbb{Q}}(B^*)$. Then by definition, for any $\mathbb{Q}-$algebra R, its $R-$points are given by

$$G_B(R) = (B \otimes_{\mathbb{Q}} R)^*$$

Then, (2.2) and (2.3) applied to G_B give us

$$G_B(\mathbb{R}) \simeq \prod_{\sigma \in \Sigma_\infty \setminus \Sigma_B} GL_2(\mathbb{R}) \times \prod_{\sigma \in \Sigma_{B,\infty}} \mathbb{H}^* \tag{2.4}$$

$$G_B(\mathbb{C}) \simeq \prod_{\sigma \in \Sigma_\infty} GL_2(\mathbb{C}) \tag{2.5}$$

Where we have that $(B \otimes_{F,\sigma} \mathbb{R})^* = (M_2(\mathbb{R}))^* = GL_2(\mathbb{R})$. Let's denote by X_B to the $G_B(\mathbb{R})-$conjugacy class of homomorphisms $\mathbb{S} \to G_{B,\mathbb{R}}$ containing

$$h_0 : \mathbb{S} \to G_{B,\mathbb{R}} \;\; s.t \;\; h_0 = \prod_\sigma h_{0,\sigma} \;\; with \;\; h_{0,\sigma}(z) = \begin{cases} z \;\; if \; \sigma \in \Sigma_\infty \setminus \Sigma_B \\ 1 \;\; if \; \sigma \in \Sigma_{B,\infty} \end{cases} \tag{2.6}$$

Observation 2.5.1. *In the previous definition, for $\mathbb{S}(\mathbb{R})$, we can identify $\mathbb{C}$ with a subring of $M_2(\mathbb{R})$ as follows*

$$a + bi \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Then the map h_0 is well defined, and we can compute it explicitly.

The isomorphisms (2.2) and (2.3) give us the identification

$$X_B = (\mathbb{P}^1)^{d_B} = (\mathcal{H}^{\pm})^{d_B}$$

with d_B being the number of infinity places of F where B is split. In this identification, we can identify the homomorphism (view as a map between matrices)

$$a + bi \to a + bi$$

with the element $i \in \mathcal{H}$

Definition 2.5.2. We define a *quaternionic Shimura variety* as $Sh_K(G_B, X_B)$ with K an open compact subgroup of $G_B(\mathbb{A}_f)$

Observation 2.5.3. *In the next section, the quaternionic Shimura variety will be given in the double coset form (we can apply proposition 2.2.12)*

$$G_B(\mathbb{Q}) \setminus (\mathbb{P}^1)^{d_B} \times G_B(\mathbb{A}_f)/K$$

Observation 2.5.4. *For the indefinite quaternionic Shimura varieties we have a canonical expression, which is*

$$\Gamma_0^B(\mathfrak{N}) \setminus \mathcal{H}^r$$

In the definite case we also have a canonical way to express those structures

$$B(\mathbb{Q})^* \setminus \mathbb{P}^{d_B} \times B(\mathbb{A}_f)^*/\hat{R}^*$$

with $\hat{R}$ the adelic complection of a maximal right order of B.

We can give some examples of K as above. Pick some integer M prime to $disc(B)$, and for other prime p which does not divide $disc(B)$, lets $e = v_p(M)$. We define $K_{0,p}$ and $K_{1,p}$ to be elements in $\mathcal{O}_p^* = GL_2(\mathbb{Z}_p)$ which are congruent to $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ and $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ $mod\ p^e$. Also we define $K_p = \mathcal{O}_p^*$ if $p \not| M$. We define

$$U_0(M) = \prod_{p \not| M} K_p \times \prod_{p|M} K_{0,p}$$

Similarly we define $U_1(M)$. Both sets are open compact subgroups of $B^*_{\mathbb{A}_f}$.

In the last section of this chapter we will analyze some Shimura variety, in this case, the quaternion algebra will be definite, this will imply that the Shimura variety will be a finite set of points, which we will identify as the ideals of the quaternion algebra.

As in all Shimura varieties, we can compute their reflex field. This case will be very similar to CM type, since in fact we are doing a higher dimensional case. Lets (G_B, X_B) be a quaternionic Shimura datum as before. By definition we have maps

$$\mathbb{S} \xrightarrow{h} G_{B,\mathbb{R}}$$

then, to obtain our cocharacter we need to obtain $h_{\mathbb{C}}$ such that makes conmutative the following diagram

$$\begin{array}{ccc} \mathbb{S}(\mathbb{R}) & \xrightarrow{h} & G_{B,\mathbb{R}} \\ \downarrow & & \downarrow \\ \mathbb{S}(\mathbb{C}) & \xrightarrow{h_{\mathbb{C}}} & G_{B,\mathbb{C}} \end{array}$$

Using the explicit definition of h by (2.6) and the observation 2.5.1, we obtain that

$$\begin{aligned} h:\ \mathbb{S} &\longrightarrow G_{B,\mathbb{R}} \\ a+bi &\rightarrow \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \overset{n}{\ldots}, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, 1, \overset{s}{\ldots}, 1\right) \end{aligned}$$

To make this diagram conmutative we select the following maps

$$\begin{aligned} \mathbb{S}(\mathbb{R}) = \mathbb{C}^* &\rightarrow \mathbb{S}(\mathbb{C}) = (\mathbb{C}\times\mathbb{C})^* \\ z &\rightarrow (z, \overline{z}) \end{aligned}$$

Looking at the first r components of G_B we have

$$G_{B,\mathbb{R}}|_{i=1,\ldots,r} \rightarrow G_{B,\mathbb{C}}|_{i=1,\ldots,r}$$
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \overset{n}{\ldots}, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \rightarrow \left(\begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}, \overset{n}{\ldots}, \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}\right)$$

Where the map is the diagonalization of the matrix over the complex numbers. The rest of the coordinates (with $1'$s we leave them fixed). Also we define

$$\begin{aligned} \mathbb{S}(\mathbb{C}) &\xrightarrow{\quad h_{\mathbb{C}} \quad} G_{B,\mathbb{C}} \\ (z_1, z_2) &\rightarrow \left(\begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}, \overset{n}{\ldots}, \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}, 1, \overset{s}{\ldots}, 1\right) \end{aligned}$$

All those definitions make the desired diagram conmutative, because the eigenvalues of the matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ are $a+bi$ and $\overline{a+bi}$. Then, the automorphisms which fix this cocharacters will be the automorphisms which fix the infinity places of F. (Because this inifinity places will give rise to embeddings (2.2) (2.3)). Then, if the automorphism fixes the cocharacter, then it respects the embeddings, and then fixes the infinity places of F.

$$E(G_B, X_B) = Fix(\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})\ s.t\ \{\infty_1, ..., \infty_r\}^\sigma = \{\infty_1, ..., \infty_r\}) \subseteq F$$

Therefore we can give more specific results depending on the quaternion algebra.

- If $B = M_2(F)$, then $r = g$ and $s = 0$ (because this quaternion algebra is a matrix group itself). Then we have that all those g matrices will act on g Poincaré half planes. Then the dimension of the Shimura variety will be g. Also, we have that the reflex field in this case is

$$E(G_B, X_B) = \mathbb{Q}$$

- If we have a quaternion algebra B such that $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R}) \times \overset{g}{\cdots} \times M_2(\mathbb{R})$. Then as before, we have g matrices such that they will act on g copies of the Poincaré half plane, giving us a Shimura variety of dimension g with

$$E(G_B, X_B) = \mathbb{Q}$$

- If we have a quaternion algebra B such that $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R}) \times \mathbb{H} \times \overset{g-1}{\cdots} \times \mathbb{H}$. We have only one group of matrices which will acts on one copy of the Poincaré half plane, making our Shimura variety of dimension 1. Also, its reflex field will be

$$E(G_B, X_B) = F$$

We also can compute its special points, lets $G = Res_{F/\mathbb{Q}}(B^*)$ with B quaternion algebra over F. Lets $E \hookrightarrow B$ be an embedding of E quadratic extension of F with at least one non-real archimedian place. Then, as we can express each point of our Shimura variety as a certain type of this embedding, we will have that $T = E^*$, giving us an special point. In the last section of this chapter, as the Gross-Zagier Shimura curve is of that type, we will use this fact as a crucial point to prove the Gross-Zagier formulae.

2.6 Automorphic forms and Jacquet-Langlands correspondence

In the previous section we have seen that quaternionic Shimura varieties, in some cases, are the higher dimensional version of modular curves. Since every modular curve has associated modular forms, it is convenient to define this type of functions on quaternionic Shimura varieties. As we will see, both maps are related by a theorem of Jacquet and Langlands. This correspondence will be a crucial part in the following chapter, and will allow us to translate quaternionic modular forms to classical modular forms and vice-versa.

First we are going to define what is an automorphic form. Classically, modular forms are functions defined as follows

$$f:\ \mathcal{H} \to \mathbb{C}$$

with some symmetry properties respect to a congruence subgroup. As we said before, we can express

$$\mathcal{H} = SL_2(\mathbb{R})/SO_2(\mathbb{R})$$

We want to generalize this concept, then, we have to change this quotient of groups by a more general construction. A priori we can see that every modular form can lift to other function

$$\widetilde{f}:\ \Gamma \setminus SL_2(\mathbb{R}) \to \mathbb{C}$$

which is invariant with respect to the $\Gamma-$action for some group Γ. This theory is defined over the Adeles, then we are going to use the Strong approximation theorem 2.1.8 without any citation along this chapter.

Definition 2.6.1. An *automorphic form* on $GL_2/\mathbb{Q}$ with grossencharacter ψ, is any function ϕ on $GL_2(\mathbb{A})$, satisfying the following conditions

1. $\phi(\gamma g) = \phi(g)$ for all $\gamma \in G_{\mathbb{Q}}$.

2. It satisfies $\phi(gz) = \phi(zg) = \psi(z)\phi(g)$, for all $z \in Z_{\mathbb{A}}$, where $Z_{\mathbb{A}}$ is the center of $\mathbb{A}$.

3. Lets $K_p = GL_2(\mathcal{O}_p)$ with $\mathcal{O}_p$ the ring of integers of $\mathbb{Q}_p$ and $K_{\mathbb{R}} = \mathcal{O}_2(\mathbb{R})$ the orthogonal group. Lets $R = K_{\mathbb{R}} \prod_{p<\infty} K_p$. Then ϕ is $R-$finite, i.e, the space of functions on $G_{\mathbb{A}}$ spanned by the right translations of $\phi(g)$ by R is finite dimensional.

4. As a function on $G_{\mathbb{R}}$, ϕ is smooth and $Z(\mathfrak{g})-$finite (with $\mathfrak{g}$ the universal enveloping algebra of G_∞).

5. For every $c > 0$ and any compact subset $T \subset G_{\mathbb{A}}$, there exist constants C, N such that

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g\right) \leq C|a|^N$$

   for all $g \in T$ and $a \in \mathbb{A}^*$ with $|a| > c$.

Also, if we have $\int_{\mathbb{Q}\backslash\mathbb{A}} \phi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) dx = 0$ for almost all g, we are going to say that ϕ is a *cusp form*.

Observation 2.6.2. *The $4-th$ condition is a generalization of the holomorphicity condition in the definition of the modular forms.*

Now we are going to see that there is a correspondence between classical cusp forms and automorphic forms.

Definition 2.6.3. If $f \in S_k(\Gamma_0(N), \psi)$, then we define

$$\phi_f(g) = f(g_{\mathbb{R}}(i))j(g_{\mathbb{R}}, i)^{-k} det(g_{\mathbb{R}})^{k/2}\psi(k_0)$$

where whe have used the Strong aproximation decomposition of $g = \gamma g_{\mathbb{R}} k_0$ with $\gamma \in G_{\mathbb{Q}}$, $g_{\mathbb{R}} \in G_{\mathbb{R}}$ and $k_0 \in K_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_p \; s.t \; c \equiv 0 \; mod \; N\mathbb{Z}_p\right\}$. Also, $j(g, z) = (cz + d)$ for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (We can see our $g_{\mathbb{R}}$ as a matrix because it is an element of $\mathcal{O}_2(\mathbb{R})$).

Proposition 2.6.4. *The map sending f to ϕ_f is an isomorphism between $S_k(\Gamma_0(N), \psi)$ and the space of functions ϕ on $G_{\mathbb{A}}$ satisfies the following properties*

1. *$\phi(\gamma g) = \phi(g)$ for all $\gamma \in G_{\mathbb{Q}}$.*

2. *$\phi(gz) = \phi(zg) = \psi(z)\phi(g)$ for all $z \in Z_{\mathbb{A}}$.*

3. *ϕ satisfies the condition (5) in the definition 2.6.1, and it is automorphic cuspidal.*

4. *This functions satisfies more conditions that scape the objective of the section. All this theory is well written at [17, p. 13].*

The proof can be found at [17, p. 13], and it uses basic theory about complex analysis and modular forms.

Observation 2.6.5. *ϕ_f is in fact an automorphic form, conditions (1), (2) and (5) are the same as in the definition of automorphic forms. The rest of conditions can be obtained using elaborated reasonings about this topic [17, p. 13].*

Since we have a relation between modular forms and automorphic forms, we also can transfer the Hecke action of the modular forms to the space of automorphic forms, in order to obtain a Hecke module. A similar reasoning will be used in the next chapter, specifically in the Eichler correspondence, and will be a key point to proof Gross-Zagier formulae.

Let's consider

$$H_p = K_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K_p$$

Then for an automorphic form ϕ on $GL_2/\mathbb{Q}$, we define

$$\widetilde{T}_p\phi(g) = \int_{H_p} \phi(gh)dh$$

We have defined automorphic forms on $GL_2/\mathbb{Q}$, we can generalize this concept to GL_2/F with F totally real field. Lets $\mathbb{A}_F$ denote the adeles ring over F.

Definition 2.6.6 (Automorphic forms for GL_2/F)**.** An *automorphic form* on GL_2/F with grossen-character ψ for F is any function ϕ on $G_{\mathbb{A}_F}$ satisfying the following conditions

1. $\phi(\gamma g) = \phi(g)$ for all $\gamma \in G_F$.
2. It satisfies $\phi(gz) = \phi(zg) = \psi(z)\phi(g)$, for all $z \in Z_{\mathbb{A}_F}$.
3. Lets $K_p = GL_2(\mathcal{O}_v)$ with v a finite place of F, and $K_{\mathbb{R}} = \mathcal{O}_2(\mathbb{R})^{|J_F|}$ the orthogonal group with J_F the set of infinite places of F. Let $R = K_{\mathbb{R}} \prod_{p<\infty} K_p$. Then ϕ is $R-$finite.
4. As a function on $G_{\mathbb{R}}$, ϕ is smooth and $Z(\mathfrak{g})-$finite (with $\mathfrak{g}$ the universal enveloping algebra of G_∞).
5. For every $c > 0$ and any compact subset $T \subset G_{\mathbb{A}_F}$, there exists constants C, N such that

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g\right) \leq C|a|^N$$

   for all $g \in T$ and $a \in \mathbb{A}_F^*$ with $|a| > c$.

Cusp forms are defined analogously.

As we said in the beginning of this section, the objective now is to define equivalent "modular forms" on Shimura varieties. The first example of a family of such functions are *Hilbert modular forms.*
Lets $\mathfrak{n} \subset \mathcal{O}_F$ be an integral ideal of F. Lets v be a finite place of F, we can define

$$K_v(\mathfrak{n}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_v \; s.t \; c \equiv 0 \; mod \; \mathfrak{n}\right\}$$

We can divide places into infinity places and into finite places using the behaviour of the field, which will be different in both cases.
Lets $K_0(\mathfrak{n}) = \prod_{v\notin J_F} K_v(\mathfrak{n})$. As the complection on the infinity places generates $GL_2(\mathbb{R})^+$, we have defined an action of $\prod_{v\in J_F} GL_2(\mathbb{R})^+$ on $\mathcal{H}_F = \mathcal{H}^{|J_F|}$. To clarify the notation from now on we are going to denote $s = |J_F|$. From the one dimensional case ($s = 1$, classical modular forms), we deduce that the stabilier of $(i, \cdots, i)$ is

$$K_{\mathbb{R}}^+ = (\mathbb{R}^* SO_2(\mathbb{R}))^s$$

We can extend the action to $GL_2(\mathbb{R})$ defining the action of $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ as follows

$$\left[\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right] \times \mathcal{H} \to \mathcal{H}$$
$$\left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, z\right) \to -\overline{z}$$

then, using the product of matrices we have the action defined for $\prod_{v \in J_f} GL_2(\mathbb{R})$.
As in the classic theory about modular forms, we can define the factor of automorphy for $\gamma \in \prod_{v \in J_F} GL_2(\mathbb{R})$, (we are going to abuse notation denoting the automorphy factor as j).

$$j(\gamma, g) = \prod_{v \in J_F} j(\gamma^v, g_v) \ for\ g = (g_v) \in \mathcal{H}_F$$

where $j(\gamma, g_v)$ are the factors of automorphy defined at 2.6.3.
The element $\overline{k} = (k_v)_v \in \mathbb{Z}^s$ is called weight vector. Lets $k_0 = max_v\ k_v$, $t_v = (k_0 - k_v)/2$ and $\overline{t} = (t_v)_v$. Also we denote by $\overline{\sigma} = \overline{k} + \overline{t} - 1$

Definition 2.6.7. An *adelic Hilbert modular form* of weight k and level $\mathfrak{n}$ is a function $f:\ G_{\mathbb{A}_F} \to \mathbb{C}$ such that

1. $f(\gamma g u) = f(g)$ for all $\gamma \in G_F$, $g \in G_{\mathbb{A}_F}$, and all $u \in K_0(\mathfrak{n})$.
2. $f(ga) = det(a)^{\overline{\sigma}} j(a, i)^{-\overline{k}} f(g)$ for all $a \in K_{\mathbb{R}}^+$ and $g \in GL_2(\mathbb{A}_F)$.
3. For $x \in GL_2(\mathbb{A}_{F,f})$ we define $f_x :\ \mathcal{H}_F \to \mathbb{C}$ by

$$f_x(z) = det(g)^{-\overline{\sigma}} j(g, i)^{\overline{k}} f(xg)$$

   where $g \in \prod_{v \in J_F} GL_2(\mathbb{R})^+$ is chosen such that $gi = z$. We can assert that this is well defined thanks to the previous statement.

4. f_x is holomorphic for all $x \in GL_2(\mathbb{A}_{F,f})$.

Also, we have defined *adelic cusp forms* in a similar way than before. For more details see [17].
We denote the space of adelic Hilbert modular forms of weight $\overline{k}$ and level $\mathfrak{n}$ by $M_{\overline{k}}(\mathfrak{n})$. Also we are going to denote by $S_{\overline{k}}(\mathfrak{n})$ the subspace of cusp forms.

We need to define finer maps, specific for each quaternion algebra B over F totally real field or $\mathbb{Q}$. We start defining some concepts for B over $\mathbb{Q}$, and then we can generalize for each F totally real field. Let's suppose that B is definite.

Lets $m \geq 0$ integer and P_m be the subspace of $\mathbb{C}[x, y]$ of homogeneous polynomials of degree m. We can define a right action of $GL_2(\mathbb{C})$ on P_m as follows; for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$. For $f \in P_m$ the action is defined as

$$\gamma \cdot f = f(dx - cy, -bx + ay)$$

Then, we denote by P_{k-2} as the module viewed as a $GL_2(\mathbb{C})-$module under this action by L_k. Since $D \otimes \mathbb{C} \simeq M_2(\mathbb{C})$, we have an isomorphism which allows us to see each element of B^* as an element of $GL_2(\mathbb{C})$. Using this observation, we have that B^* acts on L_k.

Definition 2.6.8. Lets B a quaternion algebra, we define the *space of quaternionic automorphic forms* of level $U_1(M)$ and weight k for B as

$$S_k^D(U_1(M)) = \{f:\ B_{\mathbb{A}}^* \to L_k\ s.t\ f(dgu) = f(g)u_\infty\ for\ d \in B^*, g \in B_{\mathbb{A}_f}\ and\ u \in U_1(M) \times B_{\mathbb{R}}^*\}$$

Observation 2.6.9. *Since we can express* $B_{\mathbb{A}}^* = \cup_{i=1}^n B^* d_i U_1(M) B_\infty^*$, *we see that* $f \in S_k^B(U_1(M))$ *is determined by its values on* $\{d_1, ..., d_n\}$.

Observation 2.6.10. *We can define Hecke operators on quaternionic automorphic forms, endowing to this space a structure of Hecke module.*

If we generalize those concepts to quaternion algebras defined over F totally real field of degree n over $\mathbb{Q}$, we can define quaternionic modular forms. Lets B be a quaternion algebra over F, as we did in the previous section, we have that

$$B_{\mathbb{R}}^* = (B_{\otimes_{\mathbb{Q}}}\mathbb{R})^* \simeq GL_2(\mathbb{R})^s \times (\mathbb{H}^*)^r$$

We substitute $\mathbb{Q}$ by F totally real field. This gives us a higher dimensional quaternionic Shimura variety, we are going to define a higher dimensional version of what we did for quaternionic automorphic forms.
We had an action of $GL_2(\mathbb{C})$ on P_m, let's twist this action by the character $\chi_t(\gamma) = det(\gamma)^t$ for $\gamma \in GL_2(\mathbb{C})$ and $t \in \mathbb{Z}$. We denote this new module by $P_m(t)$. Let $\overline{k} = (k_v)_v \in \mathbb{Z}^s$, using the previous notation we define

$$L_{\overline{k}} = \bigotimes_{v \in places\ where\ B\ does\ not\ split} P_{m_v}(t_v)$$

with the convention that $L_{\overline{k}} = \mathbb{C}$ if B splits over all its infinity places.
For each infinity place v on which B does not split, we choose a map

$$D \hookrightarrow D \otimes_{\mathbb{F}} \mathbb{C} \simeq M_2(\mathbb{C})$$

For any $d \in B$, lets denote by d_v the image of d under the previous embedding. Then, using the previous action, we can make $L_{\overline{k}}$ a B^*-module by sending $d \to (d_v)_v \in GL_2(\mathbb{C})^r$. Lets $P \in L_{\overline{k}}$ and $d \in B^*$, we are going to denote by P^d the action of d on P.
Now we can define an action of B^* on the space of functions

$$f: \mathcal{H}_{\pm}^s \times B_{\mathbb{A}_f}^*/U^* \to L_{\overline{k}}$$

with $U^* = \mathcal{O}(\mathfrak{n}) \otimes \hat{\mathbb{Z}}$ where $\mathcal{O}(\mathfrak{n})$ is an Eichler order of level $\mathfrak{n}$ with $\mathfrak{n}$ coprime to $disc(B)$. The action is defined for functions of this type that also satisfies

$$(f|_{\overline{k}}d)(z,u) = \left(\prod_{v \in J_F^s} \frac{det(d_v)^{\sigma_v}}{j(d_v, z_v)^{k_v}} \right) f(dz, du)^d$$

Where J_F^s is the set of all infinity places where B splits, and z_v is defined as $z_v = g_v(i, ..., i)$ with $g \in B_{\mathbb{R}}^*$ such that $g(i, ..., i) = z$.

Observation 2.6.11. *On the places where the quaternion algebra splits we have the usual transformation factor, as with Hilbert modular forms. On the places where the quaternion algebra is ramified is where we have introduced a new action.*

Definition 2.6.12. A *quaternion modular form* of weight $\overline{k}$ and level $\mathfrak{n}$ for B is a function

$$f: \mathcal{H}_{\pm}^s \times B_{\mathbb{A}_f}^*/U^* \to L_{\overline{k}}$$

which is holomorphic in the first variable and locally constant in the second, such that $f|_{\overline{k}}d = f$ for all $d \in B^*$. We denote the space of quaternionic modular forms by $M_{\overline{k}}^B(\mathfrak{n})$.

Observation 2.6.13. *As we can observe, in this definition we request an holomorphcity condition in contrast with the previous definition where we do not request this sort of condition. This is because in the definition 2.6.8, our quaternion algebra was definite, then* $s = 0$ *and we had nothing in our first variable.*

To define the cusp forms, we will have two cases

- When B is definite, we will have that $B = M_2(F)$, and then $f \in S_{\underline{k}}^D(\mathfrak{n})$ if $f(z, U^*) \to 0$ when $z \to cusp\ in\ \mathbb{P}^1(F)$.
- When B is indefinite, as there are no cusps, we have that $S_{\underline{k}}^D(\mathfrak{n}) = M_{\underline{k}}^D(\mathfrak{n})$.

We can state the main theorem of this section, the Jacquet-Langlands correspondence. We state a concrete realization of this correspondence, in terms of quaternionic modular forms, although the original theorem is stated in the languaje of automorphic representation. We will not prove this theorem, since its proof uses a deep knowledge of automorphic representation, anyway, we can found its proof in the theorem [2, thm. 16.1].

Theorem 2.6.14 (Eichler, Jacquet-Langlands, Shimizu)**.** *Lets B be a quaternion algebra over F totally real field of discriminant $\mathfrak{D}$. Lets $\mathfrak{N}$ be an ideal coprime to $\mathfrak{D}$. Then there is an injective map of Hecke modules*

$$S_2^B(\mathfrak{N}) \hookrightarrow S_2(\mathfrak{D}\mathfrak{N})$$

whose image consists of those Hilbert cusp forms which are new at all primes $\mathfrak{p}|\mathfrak{D}$.

Observation 2.6.15. *This correspondence is usually used to translate problems about modular forms between two quaternion algebra. As an example, if we take $\mathfrak{D} = 1$, we have an isomorphism*

$$S_2^B(\mathfrak{N}) \simeq S_2(\mathfrak{N})$$

we can take other quaternion algebra B', with $\mathfrak{D}' = 1$ and, using Jacquet-Langlands we obtain

$$S_2^{B'}(\mathfrak{N}) \simeq S_2(\mathfrak{N})$$

If we combine both expressions, we have a bijective correspondence between modular forms of two quaternionic Shimura varieties

$$S_2^B(\mathfrak{N}) \simeq S_2(\mathfrak{N}) \simeq S_2^{B'}(\mathfrak{N})$$

This correspondence is used by Gross to obtain the expression of $L-$functions. He solves a modular forms problem by solving a quaternionic modular forms problem. This way is simpler due to the election of a definite quaternion algebra, which gives a finite point geometry to the Shimura variety.

2.7 Gross-Zagier Shimura curve

In this section we are going to construct a Shimura curve which in the next section will allow us to express the $L-$function in terms of its special points. This variety will be a definite quaternionic Shimura variety, therefore we are going to construct this variety as we did in the section 5. We are going to study this variety in detail, obtaining interpretations of its structure. Special points of this variety will be used in the next chapter to express properties about optimal embeddings. Those properties and interpretation, will be used in the next chapter to translate the behaviour of this Shimura variety to properties about modular forms and $L-$functions.

We are going to construct a quaternionic Shimura curve. Lets B be a quaternion algebra over $\mathbb{Q}$ which ramifies at ∞ and N, then B is definite. Also we can deduce that $Res_{\mathbb{Q}/\mathbb{Q}}B^* = B^*$. This algebraic group will be part of our Shimura datum. We denote its idele points as $B(\mathbb{A})$. For every order in a quaternion algebra, we can obtain its *local component*, $R_p = R \otimes \mathbb{Z}_p$ for a prime number p. This module is defined in $B_p = B \otimes \mathbb{Q}_p$. Using this definition we can obtain the adèle complection for R as $\hat{R} = R \otimes \hat{\mathbb{Z}} = \prod_p R_p$. Throughout this section we will obtain an interpretation for this adèlic definition. It will allows us to see special points of our Shimura curve in many different ways. Lets R be a maximal order.

We are going to study the Shimura variety attached to the Shimura datum $(G_B = B^*, X_B = (\mathbb{P}^1)^{d_B=1})$. Since $\hat{R}$ is an open compact subset of $B(\mathbb{A})^*$, then we can express our Shimura variety using 2.2.12

$$X = K \setminus G_B(\mathbb{A}) \times (\mathbb{P}^1)^{d_B=1}/G_B(\mathbb{Q}) = \hat{R}^* \setminus B(\mathbb{A})^* \times \mathbb{P}^1/B^*(\mathbb{Q})$$

From now on, for simplicity, we are going to denote by $\hat{B} = B(\mathbb{A})$, and $B(\mathbb{Q}) = B$.

First, we are going to examine the right part of the Shimura variety, to obtain an interpretation of each equivalence class. We denote by $Z = \hat{R}^* \setminus \hat{B}^*/B^*$ this double quotient. Since we are using the adèle complection of the quaternion algebra B, we are going to examine it coordinate by coordinate. The local ideals of the quaternion algebra are principal, and this gives us a way to see how are the elements of this object.

Lets $I_p = R_p g_p$ with $g_p \in B_p^*/R_p^*$ local ideal. The adèlic points of the multiplicative group of the quaternion algebra is, by definition, the product of their local coordinates. Then we can see elements of Z as follows, $g_I \in \hat{B}^*/\hat{R}^*$ is of the form $(..., g_p, ...)$ with g_p in the $p-$th position. Given such point, using its coset form, we can obtain a $\mathbb{R}-$left ideal of B as follows

$$I = \hat{R}g_I \cap B$$

Then we have obtained a relation between equivalence classes of Z and ideals of B

$$\{\textit{Equivalence classes of } Z\} \to \left\{ \begin{matrix} \textit{Left R-ideals of} \\ \textit{the quaternion algebra B} \end{matrix} \right\}$$

This relation will allow us to see a coordinate of our Shimura curve as a left $R-$ideal of B.

Using an equivalence definition of *class number* for quaternion algebras, we see that left ideal classes correspond to orbits of B^* acting on the right of $\hat{B}^*/\hat{R}^*$, then the class number is $n = |\hat{R}^* \setminus \hat{B}^*/B^*|$, and it is finite due to Borel's theorem 2.1.5.
The *class number* is the number of ideals with which you can divide the algebra. Using other time Borel's theorem 2.1.5 we can obtain a new expression for the adelic points of the quaternion algebra group. We take an ideal from each equivalence class making a decision of cosets representatives of $\hat{B}^*/\hat{R}^*$. Let $g_1, ..., g_n$ the representatives, we express $\hat{B}$ as

$$\hat{B}^* = \cup_{i=1}^n \hat{R}^* g_i B^*$$

Similar to what we did with the algebra B, the right order of I_i is $R_i = B \cap g_i^{-1}\hat{R}g_i$. Using that maximal orders in B are locally conjugate in $\hat{B}$, and the subgroup which fixes R is the normalizer of $\hat{R}$; $N\hat{R}^*$, we can compute the *type number* for the adèlic complection of our algebra, $t = |B(\mathbb{Q})^* \setminus B(\mathbb{A})^*/N\hat{R}^*|$.

Observation 2.7.1. *Lets $x \in Z$, we know that x has associated an $R-$ideal I, and also we can obtain its right order. We will see in the next chapter that there is an equivalence between right orders of a quaternion algebra and supersingular elliptic curves over a finite field. In the following theory it is important to know that there are equivalent definitions from the point of view of the elliptic curves, and if we have a problem with the algebraic point of view, we can move our problem to a question about elliptic curves.*

Points as optimal embeddings

As we defined in the first chapter, when we have an optimal embedding $f : O \hookrightarrow R_i$, we have a field homomorphism $f : K \hookrightarrow B$. With this map we can define an adèlic equivalent definition

$$f(K) \cap g_i^{-1}\hat{R}g_i = f(O) \textit{ in } B(\mathbb{A})$$

with g_1 the representative of R_i. We can see that this definition involves the choice of cosets $\{g_i\}$ and the map f. Also we observe that the adèle optimal embeddings which are contained in $\widehat{R}^* \setminus Hom(K,B) \times \hat{B}^*/B^*$. B^* act on the right of this set by $(g,f) \to (gb, b^{-1}fb)$. Using that $\hat{B}^* = \cup \hat{R}g_iB^*$, the set of all optimal embeddings modulo conjugation by R_i^* is identified with the classes of the quotient $U(K) = (\widehat{R}^* \setminus \widehat{B}^* \times Hom(K,B))/B^*$ which (g,f) satisfies $f(K) \cap g^{-1}\hat{R}g = f(O)$.

We can observe that this new object $U(K)$ are the points of a Shimura curve U over K, where we have used $D = Hom(K,B)$ (with the action defined), later we are going to see that this is the same Shimura variety defined before in this section. This variety is well defined because when we define D, we have to find the following homomorphism

$$h : \mathbb{S} \to B_{\mathbb{R}}$$

$Hom(K,B)$ are those homomorphisms, which generates our hermitian symmetric domain D. As we said before, $\widehat{R}$ is a compact subset of $\widehat{B}$ with the adelic topology, and $B(\mathbb{Q}) = B$, then we can use 2.2.12 to construct our Shimura curve U.
We know that $U(K)$ are the $K-$rational points of a Shimura variety U, because $Hom(K,B)$ are defined over $K \subset \mathbb{S}(\mathbb{R})$.

Observation 2.7.2. *If we have an optimal embedding $f:\ K \hookrightarrow B$ with the usual definition, we also have that f is an optimal embedding with the adèlic definition. This also works in the other way.*

Definition 2.7.3. Lets B be quaternion algebra, we define the *space of pure quaternions* as $B^0 = \{\alpha \in B : trd(\alpha) = 0\}$.

Observation 2.7.4. *If we restrict the nrd to B^0 with $B = (a,b|K)$, we have $nrd|_{B_0}(xi+yj+zk) = -ax^2 - by^2 + abz^2$. We observe that $nrd|B_0 = 0$ defines a curve of genus 0 over the projective plane.*

Theorem 2.7.5. *Lets F be a field with char $F \neq 2$. The functor $B \to nrd|B^0$ yields an equivalence of categories between*

$$\left\{\begin{array}{c}\textit{Quaternion algebras over F, under}\\ \textit{F-algebra siomorphism, and anti-isomorphims}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Ternary quadratic forms over } F\\ \textit{with discriminant } 1 \in F^{\times}/F^{\times 2}\\ \textit{under isometries.}\end{array}\right\}$$

We can use this theorem in order to relate X with U. Lets B be our quaternion algebra defined over $\mathbb{Q}$. By the previous theorem we have a curve of genus 0 associated, which we are going to denote by Y. We define points of Y in any $\mathbb{Q}-$algebra E as

$$Y(E) = \{\alpha \in B \otimes E :\ \alpha \neq 0,\ trd(\alpha) = 0,\ nrd(\alpha) = 0\}/E^*$$

Using the correspondence

$$\left\{\begin{array}{c}\textit{Points over } R \textit{ of an}\\ \textit{algebraic variety}\end{array}\right\} \longleftrightarrow \{Spec(R)\}$$

if A is a $K-$algebra, we can express the $A-$rational points as

$$Y(A) = Hom(Spec(A) \to Spec(R)) = Hom(R \to A)$$

Thus, we can obtain the following expression for $Y(K)$.

$$Y(K) = Hom(K,B)$$

For each embedding $f : K \hookrightarrow B$, we are going to say that $y = y_f$ is the image of the unique $K-$line on the quadric $\{\alpha \in B \otimes K : \ trd(\alpha) = 0, \ nrd(\alpha) = 0\}$ on which conjugation by $f(K^*)$ acts by multiplication by $k/\overline{k}$.

Now, we can express U in terms of a genus 0 curve,

$$U = \hat{R}^* \setminus \hat{B}^* \times Y/B^*$$

Every genus 0 curve is isomorphic to the projective line, then

$$U = \hat{R}^* \setminus \hat{B}^* \times Y/B^* = \hat{R}^* \setminus \hat{B}^* \times \mathbb{P}^1/B^* = X$$

giving us that $U = X$.

Using 2.2.24, we have an isomorphism which takes $\hat{R}^* g_i \times y \ (mod \ B^*)$ to the coset $y \ (mod \ \Gamma_i)$. Then we can rewrite the curve as

$$X \simeq \cup_{i=1}^{n} Y/\Gamma_i$$

With this expression we can see our curve as the disjoint union of n curves of genus 0 (modulo some groups).

Since we have expressed our Shimura curve with optimal embeddings, now we are going to obtain some properties of this Shimura curve. This properties will help us in the next chapter to obtain the expressions of the $L-$functions.

Proposition 2.7.6. *Special points of X over K are the image of any point of $\hat{R} \setminus \hat{B} \times Y(K)$ in $X(K)$.*

Proof. For every point $x \in D$ there exists a map $h_x : \ K \hookrightarrow B$. Then, since each special point is defined by an optimal embedding $K \hookrightarrow B$, the map h_x will be this embedding. Aso the torus for each point will be $Res_{K/\mathbb{Q}} K^* = K^*$. Then we have that $h_x(\mathbb{C}^*) = h_x(K^*) \subset K^*$. We have that every point $x \in D$ is a special point with K^* as a torus. ∎

Observation 2.7.7. *We can see special points $x \in X$ as $x = g \times y$ such that $g \in Z = \hat{R}^* \setminus \hat{B}^*/B^*$ and $y \in Y(K)$, i.e, y is an homomorphism $f : \ K \hookrightarrow B$.*

Definition 2.7.8. We say that the point $x = g \times y$ has *discriminant* d if $f(K) \cap g^{-1}\hat{R}g = f(O)$ is the image of an order of discriminant d where f is the embedding which we have associated to y.

We can divide our curve X in finite components, as we divided Z. Lets $x = g \times y$, x we say that x lies in the component $X_i(K)$ if $g \equiv g_i \in \hat{R}^* \setminus \hat{B}^*/B^*$. There are $h_i(d)$ special points of discriminant d in the $i-$th component (modulo conjugation), because there are the same points as maps such that $f(K) \cap g^{-1}\hat{R}g = f(O)$. This is the number of optimal embeddings $f : \ O \hookrightarrow R_i$. (We have shown that there is an equivalence between these two types of optimal embeddings).

Special point's action
Lets $x \in X$ a special point of discriminant d, then $x = g \times y$. There exists $f : \ K \hookrightarrow B$ an embedding associated to y, this induces the natural homomorphism $\hat{f} : \ \hat{K}^* \to \hat{B}^*$.
We define the action of $a \in \hat{K}^*$ applied to x as

$$x_a = g\hat{f}(a) \times y$$

Proposition 2.7.9. *The action is well defined independent of the choice of representative for x. Also x_a has discriminant d if and only if x has discriminant d.*

Proof. If $x \equiv g' \times y'$, since g belongs to the same ideal as g, we have that $g' = gb$ and $f' = b^{-1}fb$. If we put this together, $g'\hat{f}'(a) \times y = gb(b^{-1}\hat{f}(a)b) \times y' = g\hat{f}(a)b \times y' \equiv x_a$.

$\hat{f}(\hat{K}^*)$ is conmutative, $f(K) \cap g\hat{f}(a)^{-1}\hat{R}g\hat{f}(a) = \hat{f}(a)^{-1}(f(K) \cap g^{-1}\hat{R}g)\hat{f}(a) = \hat{f}(a)^{-1}f(O)\hat{f}(a) = f(O)$ with O order with discriminant d. ∎

Observation 2.7.10. *Subgroups K^* and $\hat{O}^*$ act trivially since $g \in \hat{R}^* \setminus \hat{B}^*/B^*$, and $\hat{f}(K^*) \in B^*$ or $\hat{f}(\hat{O}^*) \in \hat{R}$.*

We conclude with the fact that if $x = x_a$, then $a \in K^*\hat{O}^*$. If we want to obtain groups which act freely, we must remove K^* and $\hat{O}^*$, obtaining $\hat{O}^* \setminus \hat{K}^*/K^* \simeq Pic(O)$. We can identify the orbit space of this action with

$$\hat{R}^* \setminus \hat{N}^*/f(\hat{K}^*)$$

where $f: K \hookrightarrow B$ is the embedding associated to the $y-$component and $\hat{N}^* = \{g \in \hat{B}^* : f(K) \cap g^{-1}\hat{R}g = f(O)\}$. Here we have used the property that says that points x_a have discriminant d. By definition we can see adèles as a the product of the local components of the initial object

$$\hat{R}^* \setminus \hat{N}^*/f(\hat{K}^*) = \prod_p R_p^* \setminus N_p^*/f(K_p^*)$$

This double coset allows us to classify the number of optimal embeddings of O_p into R_p modulo conjugation by R_p^*. This number is 1 for all $p \neq N$, and for $p = N$ is $0, 1, 2$ depending on the behaviour of N in O. This gives a proof of

$$\sum_{i=1}^{n} h_i(d) = \begin{cases} (1 - (\frac{d}{N}))h(d) & if\ d \neq N^2 d'. \\ 0 & if\ d = N^2 d'. \end{cases}$$

Equivalent definition of points of discriminant d

If we have a point $x \in X$ such that $x = g \times y$ and $g \equiv g_i$, we can see it as an optimal embedding $f: O \hookrightarrow R_i$. Lets A be an ideal of K, this ideal takes the form $A = K \cap a\hat{O}$ with a adèle mod $\hat{O}^*$. Lets R' be the right order of R_iA. The map f induces an optimal embedding $f_a: O \hookrightarrow R'$ which corresponds to the point x_a.

We can ask how the Galois group of the extension $K/\mathbb{Q}$ acts on the curve X. If $x \in X$, x can be written as $x = g \times y$, with y corresponding to an optimal embedding $f: O \hookrightarrow R_i$. Lets $\alpha \in Gal(K/\mathbb{Q})$, we define the action as $\alpha(x) = h$ with $h = g \times \mathfrak{f}$, where

$$\begin{aligned} \mathfrak{f}: O &\to R_i \\ a &\to f(\alpha(a)) \end{aligned}$$

When N is inert in O then the group $Gal(K/\mathbb{Q}) \times Pic(O)$ acts simply transitively on the points of discriminant d. When N is ramified in O, the group $Pic(O)$ acts simply transitively. We have $x = \alpha(x)$ if and only if x corresponds to an embedding $f: O \to R_i$, where $f(\alpha(a)) = jaj^{-1}$ with j 4th root of unity in R_i^*.

Theorem 2.7.11. *There exists an embedding $f: K \hookrightarrow B$ if and only if $\forall p \in Ram(B)$, $(\frac{-D}{p}) \neq 1$.*

Proposition 2.7.12. *There are not embeddings of real quadratic fields into definite quaternion algebras.*

If we combine these two theorems with the part about quadratic fields, we can deduce that in the cases with which we are working, the action of $Gal(K/\mathbb{Q}) \times Pic(O)$ is simply transitive.

Chapter 3

Gross-Zagier formulae

3.1 Brandt matrices

In this section we will give the definition and some properties about Brandt matrices, these objects arise when we want to know how many elements of a given norm are in a quaternion algebra. Even though the definition is purely algebraic, this matrix will allow us to describe the action of Hecke operators over certain modular forms spaces. This section will be used in the next section as a glue, making easier some computations and proofs.
In this section, we will use the theory that we have defined in the first chapter about quadratic fields and quaternion algebras. One of the main tools of this theory will be the Eichler mass formula, which is proved in [1, thm. 26.1.5]. Its proof uses advanced theory of quaternion algebras from an analytic point of view.

We can subdivide each quaternion algebra B by its left ideals, as in the classical theory of number fields. We define the equivalence relation similarly; $I \sim J$ if and only if there exist $b \in B^*$ such that $J = Ib$. We can find in [1] that the set of left ideal classes is finite, with order n (*class number*). Let's choose an ideal representing each equivalence class, denoted by $\{I_1, ..., I_n\}$. By convention let $R = I_1$.

We want to do the same with orders. Lets R_i be the right order of I_i. Since our set of ideals represents all ideal classes, their right orders represent all conjugacy classes of orders in B.
We can see that if two ideals I_1 and I_2 are in a different class, it is possible that $O_R(I_1) \neq O_R(I_2)$. The number of conjugacy classes of orders in B (t, *type number*) is less or equal than the class number, i.e, $t \leq n$.

Theorem 3.1.1 (Eichler mass formula). *Let $\Gamma_i = R_i^*/\mathbb{Z}^*$ and $w_i = |\Gamma_i|$:*

$$\sum_{i=1}^{n} \frac{1}{w_i} = \frac{N-1}{12}$$

Proposition 3.1.2. *$M_{ij} = I_j^{-1} I_i = \{\sum a_k b_k : \ a_k \in I_j^{-1}, \ b_k \in I_i\}$ is a left ideal of R_j with right order R_i.*

For every $b \in M_{ij}$, we define its *reduced norm* as $n(b)/n(M_{ij})$ with $n(M_{ij})$ the unique number such that all the quotients are integers with non common factors.
We associate a set of series f_{ij} to this construction

$$j_{ij} = \frac{1}{2w_j} \sum_{b \in M_{ij}} e^{2\pi i (n(b)/n(M_{ij}))\tau}$$

We can reorder this serie in order to obtain its Fourier expansion.

$$f_{ij} = \sum_{m \geq 0} B_{ij}(m) q^m \text{ with } q = e^{2\pi i \tau}$$

The aim of these two sections will be study the matrix that defines the coefficients $B_{ij}(m)$. It is called *Brandt matrix of degree m*. Each coefficient $B_{ij}(m)$ represents the number of elements in B with reduced norm m.
We can easily compute the Brandt matrix of level 0 and 1. As we have defined the norm of the quaternion algebra as $nrd(\alpha) = \alpha\overline{\alpha}$, the only element with norm 0 is the 0, and it is contained in all M_{ij}, then we have

$$B(0) = 1/2 \begin{pmatrix} 1/w_i & ... & 1/w_n \\ : & ::: & : \\ 1/w_1 & ... & 1/w_n \end{pmatrix}$$

Using the definition of I_j^{-1} and the definition of norm, we can deduce that $B(1) = I_{n\times n}$.
In order to obtain some properties of the Brandt matrix, we need to use theory of quadratic fields. We are going to relate quadratic orders and quaternion orders via *optimal embeddings*.

With the definition of *optimal embedding*, we can relate the theory of orders of quadratic fields and quaternion algebras with the aim to give a formula for the trace of the Brandt matrix.

Lets d be a negative discriminant, lets K be the quadratic field of discriminant d and $u(d)$ the cardinal of the group of unities computed at 1.1.4. Lets $h(d) = |Pic\ O_K|$ ($Pic\ O_K$ defined with the usual equivalence relation between the ideals of O_K).
For $D > 0$ we define

$$H(D) = \sum_{df^2=-D} h(d)/u(d)$$

This sum has this form because we want to add fractions $h(d)/u(d)$ such that there exists a quadratic field with a quadratic order of discriminant $-D$.

We define the *modified invariant* $H_N(D)$

$$H_N(D) = \begin{cases} 0 \text{ if } N \text{ splits in } O_{-D} \\ H(D) \text{ if } N \text{ is inert in } O_{-D} \\ 1/2H(D) \text{ if } N \text{ is ramified in } O_{-D} \text{ but } N \text{ does not divide the conductor of } O_{-D} \\ H_N(D/N^2) \text{ if } N \text{ divides the conductor of } O_{-D} \end{cases}$$

with O_{-D} the ring of integers of the quadratic field of discriminant $-D$.

Proposition 3.1.3 (Eichler trace formula)**.** *For all $m \geq 0$*

$$Trace(B(m)) = \sum_{s\in\mathbb{Z},\ s^2\leq 4m} H_N(4m - s^2)$$

Proof. For $m = 0$ we have computed the matrix. We can apply the mass formula and obtain the result.

Using the definition of the Brandt matrix, $B_{ii}(m) = \#\{b \in M_{ii}\ s.t\ n(b)/n(M_{ii}) = m\}$. We define sets

$$A_i(s,m) = \{b \in R_i\ s.t\ trd(b) = s,\ nrd(b) = m\}$$

The algebra B is ramified at ∞, this implies that $a, b < 0$, then the discriminant of any element is < 0. $A_i(s,m) = \varnothing$ if $s^2 > 4m$. Using this property, we can write the trace of the matrix as

$$Trace(B(m)) = \sum_{i=1}^{n} \sum_{s^2\leq 4m} \frac{\#A_i(s,m)}{\#R_i^*} = \sum_{s^2\leq 4m} (\sum_{i=1}^{n} \frac{\#A_i(s,m)}{\#R_i^*})$$

We claim that $\sum_{i=1}^{n} \frac{\#A_i(s,m)}{\#R_i^*} = H_N(4m - s^2)$. When $4m - s^2 = 0$, the problem is fulfilled thanks to the mass formula. From now on, we are going to suppose that $D = 4m - s^2$ is positive.

For all $b \in A_i(s,m)$, we construct the quadratic order $\mathbb{Z} \oplus b\mathbb{Z} = O_{-D}$. Using that $trd(b^2) = b^2 + \overline{b^2} = b^2 + \overline{b}^2 = (b + \overline{b})^2 - 2b\overline{b} = s^2 - 2m$, we compute its discriminant as

$$disc(O_{-D}) = \begin{vmatrix} 2 & s \\ s & s - 2m \end{vmatrix} = s^2 - 4m = -D$$

Using this computation, we have proved that every element which belongs to $A_i(s,m)$, also belongs to the quadratic order O_{-D}. This implies that every $b \in A_i(s,m)$ generates an embedding

$$O_{-D} \hookrightarrow R_i$$

Now, we are going to count elements of $A_i(s,m)$ as embeddings.
The group of units of R_i, $\Gamma_i = R_i^*/\{\pm 1\}$, acts on $A_i(s,m)$ by conjugation. Then orbits of Γ_i correspond to embeddings of O up to conjugation.
For $d < 0$, $h_i(d)$ is the number of optimal embeddings of the order with discriminant d into R_i, modulo conjugation by R_i^*. We conclude with

$$|A_i(s,m)/\Gamma_i| = \sum_{df^2 = -D} h_i(d)$$

The idea behind this relation is that we are searching for fields which have suborders of discriminant $-D$. This will allow us to count the number of elements of our set $A_i(s,m)$. This counts all the embeddings because if one embedding $O \hookrightarrow R$ is not optimal, then there exists S such that $O \subset S$ with $S \hookrightarrow R$ be an optimal embedding.
The order of the stabilizer of an element $b \in A_i(s,m)$ under Γ_i is equal to 1 unless the generated embedding extends to $\mathbb{Z}[\mu_6]$ or $\mathbb{Z}[\mu_4]$, with orders 3 and 2 respectively. This coincides with the cardinality of the groups of units at 1.1.4. Then

$$|A_i(s,m)| = w_i \sum_{df^2 = -D} h_i(d)/u(d)$$

Eichler calculated the value of $\sum_{i=1}^{n} h_i(d)$ as

$$\sum_{i=1}^{n} h_i(d) = \begin{cases} (1 - (\frac{d}{N}))h(d) & if\ d \neq N^2 d'. \\ 0 & if\ d = N^2 d'. \end{cases}$$

The Legendre symbol which appears in the previous formula, allows us to connect this result with the fact that N is ramified, inert or splits using 1.1.3.
Now, in order to compute the value of this sum, we are going to consider case by case.

1. If N splits in O_{-D}, this implies by 1.1.3 that $(\frac{d}{N}) = 1$. Then due to the result of Eichler, $\sum_{i=1}^{n} h_i(d) = 0$. We obtain that $\sum_{i=1}^{n} \frac{|A_i(s,m)|}{2w_i} = 0$.
2. If N is inert in O, this implies that $(\frac{d}{N}) = -1$, and then $\sum_{i=1}^{n} h_i(d) = 2h(d)$. We substitute this in the sum and then, we have that $\sum_{i=1}^{n} \frac{|A_i(s,m)|}{2w_i} = H(D)$
3. If N is ramified in O but does not divide the conductor of O_{-D}, then $\sum_{i=1}^{n} h_i(d) = h(d)$. We conclude with $\sum_{i=1}^{n} \frac{|A_i(s,m)|}{2w_i} = \frac{1}{2}H(D)$.
4. If N is ramified and divides the conductor of O_{-D}, then we have that we can reduce the equalities $df^2 = -D$ to $d(f/N)^2 = -D/N$. Thus we have that $\sum_{i=1}^{n} \frac{|A_i(s,m)|}{2w_i} = H_N(D/N^2)$.

Using these equalities we conclude that $\sum_{i=1}^{n} \frac{|A_i(s,m)|}{2w_i} = H_N(D) = H_N(4m - s^2)$. ∎

3.2 Supersingular elliptic curves

This section points out the relation between supersingular elliptic curves and orders in a quaternion algebra, this bijection will be used over the dissertation, it will allow us to carry problems about elliptic curves to problems about quaternion algebras and vice-versa. This connects with Brandt matrices because we can define maps between supersingular ellitptic curves as certain elements of a quaternion algebra. With this theory we can see that Brandt matrices contain some information about the elliptic curves, more specific about their automorphism classes.

Definition 3.2.1. An elliptic curve is called *supersingular* if

$$E[p^r] = \{0\} \text{ for all } r \geq 1$$

Theorem 3.2.2 (Deuring)**.** *Lets K be a perfect field of characteristic p and E/K an elliptic curve. Lets ϕ_r be the p^r-Frobenius map and $\hat{\phi}_r$ its dual. The following statements are equivalents:*

1. *E is a supersingular elliptic curve.*
2. *$\hat{\phi}_r$ is inseparable for all $r \geq 1$.*
3. *The map $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*
4. *$End(E)$ is an order in a quaternion algebra ramified at p at ∞.*
5. *The formal group $\hat{E}/K$ associated to E has height 2.*

Proof. Since the Frobenius map is purely inseparable, then we have

$$deg_s(\hat{\phi}_r) = deg_s[p^r] = (deg_s[p])^r = (deg_s\hat{\phi})^r$$

Using [7, III, 4.10 a], we can relate

$$|E[p^r]| = deg_s(\hat{\phi}_r) = deg_s(\hat{\phi})^r$$

Then we have the equivalence between (1) and (2).
Now we can express the degree of the map using heights, as ϕ is purely inseparable, then

$$deg_i\hat{\phi} = (deg_i[p])/p = p^{ht(\hat{E})-1}$$

We know that $\hat{\phi}$ has degree p, showing that 2 and 5
From now on, we are going to prove the chain of implications $(2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (2)$.
If we suppose 2, then we have that $[p] = \hat{\phi} \circ \phi$ is purely inseparable. Then, we must show that $j(E) \in \mathbb{F}_{p^2}$. Using that $\hat{\phi}$ is purely inseparable, $\hat{\phi}$ factors as

$$\begin{tikzcd} E^{(p)} \arrow[r, "\hat{\phi}"] \arrow[d, "\phi'"] & E \arrow[d, "\psi^{-1}"] \\ E^{(p^2)} \arrow[r, "id"] & E^{(p^2)} \end{tikzcd}$$

where ϕ' os the $p-$th powe Frobenius map on $E^{(p)}$ and ψ has degree 1. Using [7, II 2.4.1] we have that ψ is an isomorphism and

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}$$

Then $j(E) \in \mathbb{F}_{p^2}$.

Now we suppose (3). Also suppose that $End(E)$ is not an order in a quaternion algebra. Using [7, III 9.4] we have that

$$\mathfrak{U} = End(E) \otimes \mathbb{Q}$$

is a number field.
Let E' be any elliptic curve isogeneous to E, let ψ be the isogeny such that

$$\psi: \ E \to E'$$

We have that $\psi \circ [p] = [p] \circ \psi$ and $[p]$ is purely inseparable on E, if we compare inseparability degrees, we obtain that $[p]$ is purely inseparable on E'. Then

$$|E'[p]| = deg_s[p] = 1$$

Using that (1) $\Rightarrow$ (3), we have that $j(E') \in \mathbb{F}_{p^2}$. Then we obtain that there are finitely many elliptic curves isogeneous to E, up to isomorphism.
Let $l \in \mathbb{Z}$ with $l \neq p$. Then l remains prime in $End(E')$ for every E' isogeneous to E. Using [7, III 6.4b], we have that

$$E[l^i] \simeq \mathbb{Z}/l^i\mathbb{Z} \times \mathbb{Z}/l^i\mathbb{Z}$$

Then we find a sequence of subgroups

$$\Phi_1 \subset \Phi_2 \subset \cdots \subset E \ with \ \Phi_i \simeq \mathbb{Z}/l^i\mathbb{Z}$$

Let E_i be the quotient of E by Φ_i. Then tere is an isogeny

$$E \to E_i$$

with kernel Φ_i. By the previous reasoning, there are only fintely many distinct $E_i's$, then we can choose $m, n > 0$ such that E_{m+n} and E_m are isomorphic. We compose this map with the projection form E_m to E_{m+n}, creating an endomorphism

$$\lambda: \ E_m \xrightarrow{proj} E_{m+n} \simeq E_m$$

The kernel of δ is cyclic of order l^n. Also l is prime in the ring $End(E_m)$, then comparing degrees we have

$$\lambda = u \circ [l^{n/2}]$$

for some $u \in Aut(E_m)$. But the kernel of $[l^{n/2}]$ is not cyclic for any $n > 0$. Then we have a contradiction, that comes from assuming that $End(\mathbb{Q})$ is not an order in a quaternion algebra.

Now we suppose (4). Also suppose that (2) is false, we are going to obtain a contradiction. By our assumption we have that $\hat{\phi}_r$ i separable for all $r \geq 1$. We are going to prove that $End(E)$ is conmutative, that will contradict the fact of being an order of a quaternion algebra.
The map

$$End(E) \to End(T_p(E))$$

with T_p the Tate-module, is injective. Suppose that $\psi \in End(E)$ goes to 0 through this map. By definition of the Tate-module we have that $\psi(E[p^r]) = 0$ for all $r \geq 1$. Then since $[p^r] = \phi_r \circ \hat{\phi}_r$ we have

$$ker \ \hat{\phi}_r \subset ker \ \psi$$

The assumption that $\hat{\phi}_r$ is separable implies that ψ factors through $\hat{\phi}_r$. Then defining the map

$$\lambda_r: \ E^{(p^r)} \to E$$

as the map that makes the diagram with $\hat{\phi}_r$ and ψ commutative. Then

$$deg \ \lambda_r = deg \ \psi / deg \ \hat{\phi}_r = p^{-r} deg \ \psi$$

Since this holds for every r and $deg \ \lambda_r$ is an integer, $\lambda_r = 0$.
Using [7, III 7.1b] we know that $T_p(E)$ is either 0 or $\mathbb{Z}_p$. Then this would imply $T_p(E)/pT_p(E) \simeq E[p]$, and then by assumption $E[p] \neq 0$ obtaining $T_p(E) \simeq \mathbb{Z}_p$. Using the injective map we have

$$End(E) \hookrightarrow End(T_p(E)) \simeq End(\mathbb{Z}_p) \simeq \mathbb{Z}_p$$

We obtain that $End(E)$ is conmutative, contradicting (4). ∎

Observation 3.2.3. *Besides this theorem, we can prove that every order R in a quaternion algebra which ramifies at p and ∞ has associated a supersingular elliptic curve E with $End(E) = R$. Then we have a bijection*

$$\left\{ \begin{array}{c} \textit{Orders in a quaternion algebra} \\ \textit{ramified at } p,\ \infty \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{Supersingular elliptic curves} \\ \textit{over a field of characteristic } p. \end{array} \right\}$$

Lets $\mathbb{F}$ be a field of characteristic N, then there exist n isomorphism classes of supersingular elliptic curves over $\mathbb{F}$, $\{E_1, ..., E_n\}$. Where, by the previous correspondence, $n =$ class number of the quaternion algebra associated.
We have that $End(E_i) = R_i$, then we can see $R-$ideals which we defined in the previous section, $I_i = O_R(I_i) = R_i$, as $I_i = \{f \in Hom(E_z, E_i)\ for\ all\ 1 \leq z \leq n\}$. The inverse of ideals are also $I_i^{-1} = \{f \in Hom(E_i, E_z)\ for\ all\ 1 \leq z \leq n\}$.
Using this point of view, we have an isomophism

$$M_{ij} \cong Hom(E_i, E_j)$$

We associate an isogeny $\phi_b :\ E_i \to E_j$ to each $b \in M_{ij}$ by the previous isomorphism. We define

$$deg\ \phi_b = n(b)/n(M_{ij})$$

Since we have a correspondence between elements of a quaternion algebra and isogenies between supersingular elliptic curves over a field of characteristic N, it is reasonable to ask us how can we transfer operations over the quaternion algebra to isogenies (as the sum, the product or the conjugation).
If we have two elements $a, b \in B$, such that a corresponds to an isogeny $\phi_a :\ E_i \to E_j$ and b to an isogeny $\phi_b :\ E_j \to E_n$, then the product ab corresponds to $\phi_a \circ \phi_b$.
The conjugation works by dual isogenies. If we have a as in the previous case $\overline{a} = \hat{\phi_a}$. It is defined in this way because the norm $a\overline{a}$, in terms of isogenies will be $\phi_a \circ \hat{\phi_a} = [deg\ \phi_a]$, and coincides by the previous definition of degree. Furthermore, the sum is the same in both sides of the correspondence.

Proposition 3.2.4. *$B_{ij}(m)$ is equal to the number of subgroup schemes C of order m in E_i such that $E_i/C \cong E_j$*

Proof. By the definition

$$B_{ij}(m) = |M_{ij}| = |\frac{\{\phi : E_i \to E_j\ s.t\ \phi\ isogeny\ with\ degree\ m\}}{\sim}|$$

with $\sim$ the equivalence relation such that $\phi \sim \phi'$ if and only if $\phi' = \alpha\phi$ with $\alpha \in R_j^*$. We can observe that this identifies two isogenies if they have the same kernel C. This kernel is a subgroup of the curve of order m, because ϕ is an isogeny of degree m. ∎

It is known that the orders R_i and R_j are conjugated in B if and only if elliptic curves E_i and E_j are conjugated by an automorphism of the field. By Deuring's theorem, we have that modular invariants of the curves lie in the field with N^2 elements, then the curves are conjugated by automorphism of the field if and only if $i = j$ or $E_i^N \simeq E_j$. Also, we have that the kernel of the Frobenius morphism $E_i \to E_i^N$ is the only subgroup of order N in E_i. This gives the following proposition

Proposition 3.2.5. *Curves E_i and E_j are conjugated by automorphism of the field if and only if $i = j$ or $B_{ij}(N) = 1$.*

This proposition shows that Brandt's matrix has some information about elliptic curves. At the last result of this chapter, we are going to proof that $\sum_k B_{ik} = 1$. This gives us two properties: Given the list of isomorphism classes of elliptic curves $\{E_1, ..., E_n\}$

- Isomorphism classes of supersingular elliptic curves are, as maximum, group together in pairs by automorphisms of the field.

- Given a class E_i, if $E_i^N \not\simeq E_j$, $\forall j \in \{1, ..., n\} \setminus i$, then $B_{ii}(N) = 1$

Proposition 3.2.6. *Given a quaternion algebra B, we can find its type number using Brandt's matrix as follows*

$$t = Trace\ B(N) + \frac{n - Trace\ B(N)}{2}$$

Proof. In this proof we are going to use the correspondence between elliptic curves and orders. $Trace\ B(N)$ is the number of orders that are not conjugated by automorphism. $n - Trace\ B(N)$ is the number of orders which are conjugated by automorphism. As we remark before, this orders will be paired, then, if we divide by 2, we will have the number of classes of this orders. When we sum, we have the type number, i.e the number of equivalence classes with the relation given by the conjugation. ∎

Proposition 3.2.7. 1. *The row sums $\sum_j B_{ij}(m) = \sigma(m)_N := \sum_{d|m,\ (d,N)=1} d$.*

2. *If $(m, m') = 1$, then $B(m)B(m') = B(mm')$.*

3. *$B(N)$ is a permutation matrix of order dividing 2 and for $k \geq 1$, $B(N^k) = B(N)^k$.*

4. *If $p \neq N$ is prime and $k \geq 2$, $B(p^k) = B(p^{k-1})B(p) - pB(p^{k-2})$.*

5. *The matrices $B(m)$ for $m \geq 1$ generate a conmutative subring $\mathbb{B}$ of $M(n, \mathbb{Z})$.*

6. *We have the symmetry relation $w_j B_{ij}(m) = w_i B_{ji}(m)$.*

7. *The conmutative algebra $\mathbb{B} \otimes \mathbb{Q}$ is semi-simple and isomorphic to the product of totally real number fields.*

Proof. 1. Using 3.2.4 we know that $\sum_j B_{ij}(m)$ is the number of subgroups of order m in E_i. Since this is multiplicative in m, we have two options

   - If $m = N^k$ the number of subgroups of order m is 1.
   - If $m = p^k$ with $p \neq N$, then the number of subgroups of order m is equal to $1 + p + p^2 + ... + p^k$.

   Then we have $\sum_j B_{ij}(m) = \sigma(m)_N$.

2. Using 3.2.4, we can read $B_{ij}(mm')$ as the number of subgroups $C_{mm'}$ of order m in E_i with $E_i/C_{mm'} \simeq E_j$. Then, we select C_m, the unique subgroup scheme of order m in $C_{mm'}$. Let $E_k = E_i/C_m$. Now let $C_{m'}$ be the image of $C_{mm'}$ on E_k. This image has order m' and $E_k/C_{m'} \simeq E_j$. As we can factor any isogeny of degree mm' uniquely, then we obtain

$$B_{ij}(mm') = \sum_k B_{ik}(m)B_{kj}(m')$$

3. Each E_i has a unique subgroup scheme C_N of order N. This subgroup is the kernel of the Frobenius map (denoted by $E \xrightarrow{Frob} E^N$). Then $B_{ij}(N) = 1$ if $E_i^N \simeq E_j$ and $B_{ij}(N) = 0$ otherwise. Then we can see $B(N)$ as a permutation matrix of order dividing 2. Since the unique subgroup of order N^k is the kernel of $E_i \xrightarrow{Frob\ N^k} E_i^{N^K}$. Then we obtain $B(N^k) = B(N)^k$.

4. We can factorize any isogeny $\phi : E_i \to E_j$ of order p^k as an isogeny $E_i \to E_k$ of degree p followed by an isogeny $E_k \to E_j$ of degree p^{k-1}. We know that this factorization is unique if the kernel of ϕ is cyclic. If the kernel is not cyclic, then $\phi = p \cdot \phi'$ with ϕ' of degree p^{k-2}. Then there are $p+1$ possible factorizations. Then we have that

$$B(p^k)_{ij} = \sum_l B_{il}(p)B_{lj}(p^{k-1}) - pB(p^{k-2})_{ij}$$

which proves the statement.

5. We can use the two previous points to obtain that $\mathbb{B}$ is generated over $\mathbb{Z}$ by the matrices $B(N)$ and $B(p)$ for $p \neq N$.

6. We can identify $Hom(E_i, E_j)$ with $Hom(E_j, E_i)$ using the duality operator. This operator preserves the degree. Also since $w_j B_{ij}(m)$ is the half part of the elements in $Hom(E_i, E_j)$ of degree m, then we have the symmetry.

7. We can define an inner product on the group

$$\mathbb{Z}^n = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$$

using the formula $\langle e_i, e_j \rangle = w_i \delta_{ij}$. This is positive definite on $\mathbb{R}^n$, then using the previous point, the matrices $B(m)$ give self-adjoint endomorphisms of $\mathbb{Z}^n$. We conclude with this statement using spectral theorem.

∎

3.3 Main result

This subsection explains an important result in the modern number theory. This formula is the computation of the special value of some $L-$functions in terms of elements of a quaternionic Shimura variety. The significance of this proof is clear since one of the objectives of the modern number theory is to understand the behaviour of $L-$functions and their connection with elliptic curves.
We start with the computation of the special value of a $L-$function using modular forms theory. We apply Rankin's method and some computations to obtain an expression of the special value. In order to reinterpret this result we define a Shimura variety which will allow us to describe those equations in terms of their points. This result is inspired in the Jacquet-Langlands correspondence; we have a problem about modular forms (we express the $L-$function in terms of modular forms), and using this correspondence we can see our problem with an easier geometry, given by a definite quaternionic Shimura variety.

One of the underline ideas is the relation between some spaces which we will use along this section. In the previous chapter we defined a correspondence between supersingular elliptic curves and orders of a quaternion algebra, now, we add to the dissertation the theory of modular forms. Using this relation we can transfer analytic concepts and tools to our Shimura variety. The glue between those correspondence are Brandt matrices since they explain us how the operators acts in both spaces.
After proving the main result, we will analyze two more $L-$functions as corollaries of the main result. In the nex sections we will obtain special values of the $L-$function associated to an elliptic curve using modular forms of weight $3/2$.

Lets $f = \sum_{m\geq 1} a_m q^m$ be a cusp form and K an imaginary quadratic field of discriminant $-D$ in which the number N is inert. We denote by O the ring of integers of K.

Definition 3.3.1. We define the *Peterson product* of f and g, both cusp forms as

$$(f,g) = \int\int_D f(z)\overline{g(z)}dxdy$$

with D the fundamental domain of the modular curve $X_0(N)$, which is generated by $\Gamma_0(N)$. It is also defined for one of them not being a cusp form.

Lets A be a fixed ideal class of O and ϵ the quadratic character of $(\mathbb{Z}/D\mathbb{Z})^*$ such that $\epsilon(p) = (\frac{-D}{p})$ with $(\frac{\cdot}{\cdot})$ the Legendre symbol.
We can associate to each ideal class a modular form of weight 1 and character ϵ as follows

$$E_A(z) = \frac{1}{2u}\sum_{\lambda\in a} q^{\mathfrak{N}(\lambda)/\mathfrak{N}(a)} = \frac{1}{2u} + \sum_{m\geq 1} r_A(m)q^m$$

where u the cardinal of the group of units divided of K (modulo ± 1). Also, in this expression a is any ideal in the class A. If we sum the series over all classes we obtain

$$E = \sum_A E_A = \frac{h}{2u} + \sum_{m\geq 1} R(m)q^m$$

where h is the class number of K. The resulting serie is the weight 1 Eisenstein serie. We observe that coefficients $R(m)$ are the number of ideals of O with norm m.

Definition 3.3.2. The $L-$function $L(f, A, s)$ is defined as

$$L(f,A,s) = \sum_{\substack{m=1\\(m,N)=1}}^{\infty} \frac{\epsilon(m)}{m^{2s-1}} \sum_{m=1}^{\infty} \frac{a_m r_A(m)}{m^s}$$

Observation 3.3.3. *The $L-$serie is the product of two Dirichlet series. The first is a modification of the Dirichlet $L-$function $L(\epsilon, 2s-1)$, and the second converges for $Re(s) > 3/2$.*

The aim of this section is to compute the value of the $L-$function at $s = 1$. First we are going to use analytic techniques, and later we are going to reinterpret this result using Shimura varieties. Now, we are going to apply the Rankin's method to obtain a functional equation for $L(f, A, s)$, and the first part of the main result will be inmediately.

Lets $\Gamma_\infty = \left\{\pm\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\ s.t\ n\in\mathbb{Z}\right\}$, we can observe that $\Gamma_\infty \subset \Gamma_0(N)\ \forall N \in \mathbb{Z}$. The fundamental domain of this subgroup is $D_\infty = \{0 \leq x < 1,\ 0 < y < \infty\}$. The idea in the following equations is to change the region of the integral to obtain the fundamental domain of $\Gamma_0(N)$. With this integrals we will be able to obtain a Peterson product.
For a large $Re(s)$

$$(4\pi)^{-s}\Gamma(s)\sum_{m=1}^{\infty}\frac{a_m r_A(m)}{m^s} = \int_0^\infty (\sum_{m=1}^{\infty} a_m r_A(m) e^{-4\pi m y}) y^s \frac{dy}{y} =$$

This equality is given by the fact that $\int_0^\infty e^{-y}(\frac{y}{m})^s a_m r_A(m)\frac{dy}{y}$ is the Mellin transform of $e^{-y}(\frac{1}{m})^s a_m r_A(m)$. In particular, the Mellin transform uses the multiplicative Haar measure $\frac{dy}{y}$, so it is multiplicative invariant and we can consider $y \to 4\pi m y$.

$$= \int_0^\infty (\int_0^1 f(x+iy)\overline{E_A(x+iy)}dx) y^s \frac{dy}{y} = \int\int_D f(z)\overline{E_A(z)}y^{s+1}\frac{dxdy}{y^2} = (\cdot)$$

The first equality comes because we do the product and use that $\int_0^\infty e^{2\pi i m x}dx = 0$ for all $m \neq 0$. Now, given Γ_1 and Γ_2 congruence subgroups such that $\Gamma_1 \subset \Gamma_2$, we can give a decomposition of

Γ_2 as $\Gamma_2 = \cup_i \Gamma_1 \alpha_i$. Let R_1 and R_2 be their fundamental domains, we can change the domain of the integral as follows

$$\int_{R_1} \phi(t)d\mu(t) = \int_{\cup \alpha_i R_2} \phi(t)d\mu(t) = \sum_{\alpha_i \in \Gamma_2/\Gamma_1} \int_{\alpha_j R_2} \phi(t)d\mu(t)$$

Applying this to the main equality we have

$$(\cdot) = \sum_{\gamma \in \Gamma_0(ND)/\Gamma_\infty} \int\int_{\gamma F_{ND}} f(z)\overline{E_A(z)}y^{s+1}\frac{dxdy}{y^2} = \sum_{\gamma \in \Gamma_0(ND)/\Gamma_\infty} \int\int_{F_{ND}} f(\gamma z)\overline{E_A(\gamma z)}Im(\gamma z)^{s+1}\frac{dxdy}{y^2} = (\cdot\cdot)$$

Now we are going to use the modular behaviour of the functions f and E_A under $\Gamma_0(ND)$.

1. $f(\gamma z) = f(z)(cz+d)^2$
2. $E_A(\gamma z) = \overline{E_A(z)}(c\overline{z}+d)\epsilon(d)$
3. $Im(\gamma z) = \frac{y}{|c\overline{z}+d|^2}$

We can also define the set $C = \left\{(c,d) \ s.t \begin{pmatrix} \cdot & \cdot \\ c & d \end{pmatrix} \in \Gamma_0(ND)/\Gamma_\infty\right\}$ to simplify the notation

$$(\cdot\cdot) = \sum_{(c,d)\in C} \int\int_{F_{ND}} f(z)\overline{E_A(z)}\frac{\epsilon(d)}{c\overline{z}+d}\frac{y^{s-1}}{|cz+d|^{2s-2}}dxdy$$

Definition 3.3.4. *Eisenstein series of weight 1* $E_{ND}(s,z)$ with character ϵ are defined as follows

$$E_{ND}(s,z) = \sum_{m=1,\ (m,N)=1} \frac{\epsilon(m)}{m^{2s+1}} \sum_{(c,d)\in C} \frac{\epsilon(d)}{cz+d}\frac{y^s}{|cz+d|^{2s}} =$$

$$= \sum_{m=1,\ (m,N)=1} \frac{\epsilon(m)}{m^{2s+1}}\frac{1}{2} \sum_{\substack{c,d\in\mathbb{Z},\ c\equiv 0\ (ND) \\ (d,ND)=1}} \frac{\epsilon(d)}{(cz+d)}\frac{y^s}{|cz+d|^{2s}}$$

Multiplying both sides of the main expression by $\sum \frac{\epsilon(m)}{m^{2s+1}}$ and switching the integral by the sum

$$(4\pi)^{-s}\Gamma(s)L(f,A,s) = \int\int_{F_{ND}} f(z)\overline{E_A(z)E_{ND}(\overline{s}-1,z)}dxdy$$

It is proved that the function $\pi^{-s}\Gamma(s)E_{ND}(s,z)$ can be continued to an entire function on the $s-$plane. This gives us the analytic continuation of $L^*(f,A,s) = ((2\pi)^{-s}\Gamma(s))^2(ND)^s L(f,A,s) = L^*(f,A,2-s)$. This follows from the behaviour of the Eisenstein series. Now, substituting $s=1$

$$L(f,A,1) = (4\pi)\int\int_{F_{ND}} f(z)\overline{E_A(z)E_{ND}(0,z)}dxdy$$

In order to change the domain of the integral we define the trace function as

$$\begin{aligned} Tr_N^M :\ & M_{2k}(\Gamma_0(N)) \to M_{2k}(\Gamma_0(M)) \\ & g \to \sum_{\gamma\in\Gamma_0(N)/\Gamma_0(M)} g|_{2k}\gamma \end{aligned}$$

Now we use the fact that $(f,g)_{\Gamma_0(M)} = (f, Tr_N^M g)_{\Gamma_0(N)}$ for any $f \in S_{2k}(\Gamma_0(N))$ and $g \in M_{2k}(\Gamma_0(M))$. Therefore, we can express our $L-$function as

$$L(f,A,1) = \frac{1}{2\pi}(f, Tr_N^{ND}\{E_A(z)E_{ND}(0,z)\})$$

We remark that the Eisenstein serie $E_{ND}(s,z)$ can be expressed in terms of the Eisenstein series $E(s,z)$ of weight 1 and level D, defined by

$$E(s,z) = \frac{1}{2} \sum_{\substack{c,d\in\mathbb{Z} \\ c\equiv 0\ (D)}} \frac{\epsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}}$$

At $s=0$, we obtain the identity

$$E_{ND}(0,z) = E(0,Nz) + N^{-1}E(0,z)$$

We observe that the second term contributes 0 to the trace. This happens because $N^{-1}E_A(z)E(0,z)$ has weight 2 and level D and then $Tr_N^{ND}(N^{-1}E_A(z)E(0,z)) = Tr_1^D(N^{-1}E_A(z)E(0,z)) = 0$. Hence

$$L(f,A,1) = \frac{1}{2\pi}(f, Tr_D^{ND}(E_A(z)E(0,Nz)))$$

Furthermore, Hecke proved that $E(0,z)$ was related to the series $E = \sum_A E_A$ by the formula

$$E(0,z) = \frac{2\pi}{\sqrt{D}} E(z)$$

We conclude with the main result of this subsection

Proposition 3.3.5. *Let $G_A(z) = Tr_D^{ND}(E_A(z)E(Nz))$. Then*

$$L(f,A,1) = \frac{(f,G_A)}{\sqrt{D}}$$

for any cusp form f of weight 2 on $\Gamma_0(N)$.

3.4 Trace computation

We are going to use the following notation

$$g = E_A(z)E(Nz) \text{ and } G_A = Tr_N^{ND} g$$

The aim of this section is to compute the Fourier coefficients of G_A of weight 2 for $\Gamma_0(N)$ for D prime. With D non prime this result is satisfied too.

$$E_A(z) = \sum_{m=0}^{\infty} r_A(m)q^m \text{ and } E(z) = \sum E_A(z) = \sum_{m=0}^{\infty} R(m)q^m$$

Lemma 3.4.1. 1. *If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ with $c \not\equiv 0$ (mod D), then*

$$E_A|_1\gamma = \frac{\epsilon(c)}{i\sqrt{D}} E_A(\frac{z+c^*d}{D})$$

where c^* is the inverse for c (mod D).

2. *If $\gamma \in \Gamma_0(N)$ with $c \not\equiv 0$ (mod D), then*

$$E(Nz)|_1\gamma = \frac{\epsilon(c)}{i\sqrt{D}} E(N(\frac{z+c^*d}{D}))$$

Proof. 1. The cosets of $SL_2(\mathbb{Z})/\Gamma_0(D)$ are matrices $\begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$ with $0 \leq j < D$. We are going to compute the action of those matrices, and later, this will help us to give the final result. We have the following decomposition of the matrix $\gamma = \frac{1}{D}\begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix}\begin{pmatrix} 1 & j \\ 0 & D \end{pmatrix}$. Applying this to E_A we have that

$$E_A|_1\gamma = E_A|_1 \begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix} |_1 \begin{pmatrix} 1 & j \\ 0 & D \end{pmatrix} = \frac{1}{i} E_A|_1 \begin{pmatrix} 1 & j \\ 0 & D \end{pmatrix}$$

where we have used that $E_A|_1 \begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix} = \frac{1}{i} E_A$ from Poisson summation. Then we conclude with

$$\frac{1}{i} E_A|_1 \begin{pmatrix} 1 & j \\ 0 & D \end{pmatrix} = \frac{1}{i\sqrt{D}} E_A(\frac{z+j}{D})$$

In the general case, as $SL_2 = \bigcup \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$ with $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(D)$ (in this case $c = \delta$ and $c^*d \equiv j \ (mod\ D)$). Applying this product of matrices to E_A and using the previous result, we have that

$$E_A|_1\gamma = (E_A|_1 \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix})|_1 \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$$

since E_A is a modular form of weight 1 and character ϵ for $\Gamma_0(D)$, we obtain that

$$E_A|_1\gamma = \frac{\epsilon(c)}{i\sqrt{D}} E_A(\frac{z + c^*d}{D})$$

2. By definition $E = \sum E_A$, using the first result of this lemma, we obtain that

$$E|_1\gamma = \frac{\epsilon(c)}{i\sqrt{D}} E(\frac{z + c^*d}{D})$$

Using the identity $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, we obtain

$$E(Nz)|_1\gamma = E|_1 \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}(Nz) = \frac{\epsilon(c/N)}{i\sqrt{D}} E(\frac{Nz + Nc^*d}{D}) = \frac{\epsilon(c)}{i\sqrt{D}} E(N(\frac{z + c^*d}{D}))$$

where we have used that $\epsilon(N) = -1$.

∎

Proposition 3.4.2. *If D is prime then*

1. $G_A(z) = g(z) + \frac{1}{D}\sum_{j=0}^{D-1} g(\frac{z+j}{D})$.
2. *If $G_A(z) = \sum_{m \geq 0} a_m q^m$, the Fourier coefficients a_m are as given by this formula*

$$a_m = \sum_{n=0}^{Dm/N} r_A(Dm - nN)\delta(n)R(n) = \frac{r_A(m)h}{u} + \sum_{n=1}^{Dm/N} r_A(Dm - nN)\delta(n)R(n)$$

where $\delta(n) = \begin{cases} 1 & \text{if } (n, D) = 1 \\ 2 & \text{if } n \equiv 0 \ (mod\ D) \end{cases}$

Proof. 1. There are $D+1$ cosets of $\Gamma(N)/\Gamma_0(ND)$. They have representatives $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ such that $c \neq 0$ $(mod\ D)$ and $j = c^* d$ runs over the D residue classes $mod\ D$.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a coset representative. Since

$$g|_2\gamma = E_A|_1\gamma E(Nz)|_1\gamma$$

we can compute

$$g|_2\gamma(z) = \frac{\epsilon(c)}{i\sqrt{D}} E_A(\frac{z+j}{D}) \frac{-\epsilon(c)}{i\sqrt{D}} E(N(\frac{z+j}{D})) = \frac{1}{D} g(\frac{z+j}{D})$$

If we sum all the cosets we obtain

$$G_A(z) = g(z) + \frac{1}{D} \sum_{j=0}^{D-1} g(\frac{z+j}{D})$$

2. If $g(z) = E_A(z)E(Nz) = \sum_{m \geq 0} b_m q^m$ and $G_A(z) = \sum_{m \geq 0} a_m q^m$, the previous result implies that $a_m = b_m + b_{mD}$ since

$$\frac{1}{D} \sum_{j=0}^{D-1} g(\frac{z+j}{D}) = \sum_{m=0}^{\infty} b_{mD} q^m$$

g is a product of series, this implies that we can express every b_m as a convolution

$$b_m = \sum_{l \geq 0} r_a(m - lN)R(l) = \sum_{\substack{n \geq 0 \\ n \equiv 0\ (D)}} r_A(mD - nN)R(n)$$

where the sums are finite. For the second equality, we set $n = Dl$. Since D is prime, there exists an unique ideal of norm D, then $r_A(k) = r_A(DK)$ and $R(k) = R(Dk)$ for $k \geq 1$. We obtain that

$$a_m = \sum_{\substack{n=0 \\ n \equiv 0\ (D)}}^{Dm/N} r_A(mD - nN)R(n) + \sum_{l=0}^{Dm/N} r_A(mD - lN)R(l)$$

we add the function $\delta(n)$, because when $(n, D) = 1$, then $r_A(mD - nN)R(n)$ appears in the second sum, but when $n \equiv 0$ $(mod\ D)$ it appears in both.

∎

3.5 Eichler correspondence

In this section we are going define an operator in $Pic(X)$ such that it acts like a Hecke operator. This will give us a correspondence between this space and the space of modular forms of weight 2, i.e, an explicit Jacquet-Langlands correspondecee. This correspondence will allow us to solve our problem due to the geometry of X. The way in which the operator acts, is given by Brandt matrices.

Since the group $Pic(X)$ will be used along this section, we will explain briefly how can we see modular forms as sections of line bundles.

Let X be a Riemann surface, we define a *line bundle* on X as a map of complex manifolds $\pi:\ L \to X$ such that locally L is isomorphic to $U \times \mathbb{C}$. We can define a *section* of a line bundle

π as a map f such that $\pi \circ f = id$. If L is a line bundle on X, for any open subset U of X, we denote the group of sections of L over U as $\Gamma(U, L)$.

Lets Γ be a group acting freely and properly discontinuously on a Riemann surface H, lets $X = \Gamma \setminus H$. We denote the canonical projection by $p : H \to X$. Lets $\pi : L \to X$ be a line bundle on X, then we define

$$p^*(L) = \{(h, l) \subset H \times L \; s.t \; p(h) = \pi(l)\}$$

This is also a line bundle on H. We can define the action of Γ on $p^*(L)$ through its action on H (for $\gamma \in \Gamma$ and $(a, b) \in p^*(L)$, $\gamma(a, b) = (\gamma(a), b)$). Lets

$$i : H \times \mathbb{C} \to p^*(L)$$

be an isomorphism. Lets $\gamma \in \Gamma$ and $(h, c) \in H \times \mathbb{C}$, we define $\gamma \cdot (h, c) = i^{-1}(\gamma(i(h, c)))$. Using this definition, we can transfer the action of Γ on $p^*(L)$ to an action on $H \times \mathbb{C}$. For any $\gamma \in \Gamma$ and $(\tau, z) \in H \times \mathbb{C}$, we express this action as

$$\gamma(\tau, z) = (\gamma\tau, j_\gamma(\tau)z) \;\; with \; j_\gamma(\tau) \in \mathbb{C}^*$$

This action is well defined because

$$\gamma\gamma'(\tau, z) = \gamma(\gamma'\tau, j_{\gamma'}(\tau)z) = (\gamma\gamma'\tau, j_\gamma(\gamma'\tau) \cdot j_{\gamma'}(z) \cdot z)$$

also, this action has a cocycle property

$$j_{\gamma\gamma'}(\tau) = j_\gamma(\gamma'\tau) \cdot j_{\gamma'}(\tau)$$

Definition 3.5.1. An *automorphy factor* is a map $j : \Gamma \times \mathcal{H} \to \mathbb{C}^*$ such that

1. for each $\gamma \in \Gamma$, $\tau \to j_\gamma(\tau)$ is a holomorphic function on $\mathcal{H}$.
2. $j_{\gamma\gamma'}(\tau) = j_\gamma(\gamma'\tau) \cdot j_{\gamma'}(\tau)$.

Example 3.5.2. *For any open subset H of $\mathbb{C}$ with a group acting on it, there exists a canonical automorphy factor $j_\gamma(\tau)$*

$$\begin{aligned} \Gamma \times H &\to \mathbb{C} \\ (\gamma, \tau) &\to (d\gamma)_\tau \end{aligned}$$

with $d(\gamma)_\tau$ the map on the tangent space at τ defined by γ. Since $H \subset \mathbb{C}$ $(d\gamma)_\tau$ is a complex number. We can use this example to connect this definitions to the theory of modular forms. Lets $\Gamma(1) \setminus \mathcal{H}$. Our γ is defined as

$$z \to \frac{az + b}{cz + d}$$

then we can define its canonical automorphy factor as

$$d\gamma = \frac{1}{(cz + d)^2} dz$$

Proposition 3.5.3. *There is a one-to-one correspondence between the set of pairs (L, i) where L is a line bundle on $\Gamma \setminus \mathcal{H}$ and i is an isomorphism $H \times \mathbb{C} \simeq p^*(L)$ and the set of automorphy factors.*

Proof. With the previous reasoning we have seen the direction $(L, i) \to j_\gamma(\tau)$. For the converse, we can define an action of Γ on $H \times \mathbb{C}$ as we did, and then define L as $\Gamma \setminus H \times \mathbb{C}$. ∎

Lets L be a line bundle on X. We define

$$\Gamma(X,L) = \{F \in \Gamma(H, p^*L) \; s.t \; F \; conmutes \; with \; the \; actions \; of \; \Gamma\}$$

Suppose that we have an isomorphism $p^*(L) \simeq H \times \mathbb{C}$, we can use it to identify line bundles on H. Γ acts on $H \times \mathbb{C}$ by the rule

$$\gamma(\tau, z) = (\gamma\tau, j_\gamma(\tau)z)$$

Lets F be a holomorphic section, it can be written as

$$\begin{aligned} F: \; H &\to H \times \mathbb{C} \\ \tau &\to (\tau, f(\tau)) \end{aligned}$$

with $f: \; H \to \mathbb{C}$ a holomorphic map. With this expression, we can rewrite the condition of $\Gamma(X,L)$ as

$$F \; conmutes \; with \; the \; actions \; of \; \Gamma \; if \; (\gamma\tau, f(\gamma\tau)) = (\gamma\tau, j_\gamma(\tau)f(\tau))$$

Hence, we have that

$$f(\gamma\tau) = j_\gamma(\tau) \cdot f(\tau)$$

Observation 3.5.4. *If L_k is the line bundle on $\Gamma \setminus \mathcal{H}$ which corresponds to $j_\gamma(\tau)^{-k}$, where $j_\gamma(\tau)$ is the canonical automorphy factor, then the condition becomes*

$$f(\gamma\tau) = (cz+d)^{2k} f(\tau)$$

Then, we can see that the sections of L_k are in natural one to one correspondence with the functions of $\mathcal{H}$ satisfying the previous equality. We can extend this sections to $\Gamma \setminus \mathcal{H}^*$, and then, we have a correspondence 1-1 between sections of a modular curve and modular forms.

Definition 3.5.5. *We define $Pic(X)$ as the set of lines bundles on X.*

Using the fact that given a genus 0 curve Y, $Y \simeq \mathbb{P}$

$$Pic(X) = Pic(\cup_{i=1}^n X_i) = \cup_{i=1}^n Pic(X_i) = \mathbb{Z}^n$$

with X_i components of the curve X. We can pick generators of $Pic(X_i)$ and form a basis such that $Pic(X) = \langle e_1, ..., e_n \rangle$.

Observation 3.5.6. *If $x \in X$, then $x \in Pic(X)$. Previously, we have related the points in X with left $R-$ideals of B. Each one of the ideals I_i belongs to the $i-th$ component of X. This gives us two points of view of the following theory; using ideals or using the Picard group.*

We can see the curve X as

$$X \simeq (\hat{R}^* \setminus \hat{B}^*/\hat{\mathbb{Q}}) \times Y/(B^*/\mathbb{Q}^*)$$

This means that points of the curve X are $g = (...g_p...)$ such that each coordinate lies in $R_p^* \setminus B_p^*/\mathbb{Q}_p^*$. When $p \neq N$, the space $R_p^* \setminus B_p^*/\mathbb{Q}_p^* \simeq PGL_2(\mathbb{Q}_p)/PGL_2(\mathbb{Z}_p)$, and this quotient has the same structure as the set of vertices in a homogeneous tree of degree $p+1$. When $p = N$, $R_p^* \setminus B_p^*/\mathbb{Q}_p^*$ has two elements. We can see this double quotient as the set of vertices in a homogeneous tree of degree 1.
Lets δ_p be the distance function on the tree at the place p, we define

$$t_m(g) = \sum_{\substack{\delta_p(g_p,h_p) \leq ord_p(m) \\ \delta_p(g_p,h_p) \equiv ord_p(m) \; (2)}} (h)$$

with (h) the element which every coordinate satisfies the distance conditions.

Proposition 3.5.7. *The operator t_m verifies the following properties*

1. *t_m is self dual.*

2. *If $(m, m') = 1$, then $t_{mm'} = t_m t_{m'}$.*

3. *If p is a prime such that B does not ramifies at p, $t_{p^{k+2}} = t_{p^k} t_p - p t_{p^k}$.*

4. *If p is a prime such that B ramifies at p, $t_{p^k} = (t_p)^k$.*

Observation 3.5.8. *t_m preserves $\hat{R}^* \setminus \hat{B}^* / \hat{Q}^*$.*

This map induces a correspondence on X

$$t_m(g \times y) = \sum_{h \in t_m(g)} (h \times y)$$

As we have seen, we can see points of Z as left $R-$ideals of B. We define the set $M(R)$ as the free $\mathbb{Z}-$module generated by $\{I_1, ..., I_n\}$. This set is in correspondence 1-1 with the elements of Z. Lets $\mathfrak{N}$ be the ideal norm. We deduce that the operator t_m in this set acts in the following way

$$t_m(I) = \sum_{\substack{J \in M(R) \ s.t \\ \mathfrak{N}(J) = m\mathfrak{N}(I)}} J$$

Observation 3.5.9. *We have a 1-1 correspondence between right orders and supersingular elliptic curves, due to Deuring. Since every left ideal has an associated right order, considering the $\mathbb{Z}-$module of supersingular elliptic curves, we can transcript the operator t_m as follows*

$$t_m[E_i] = \sum_{j \in \lambda} [E_j]$$

where $\lambda = \{E_j \ s.t \ \exists \phi \in Hom(E_i, E_j)/Aut(E_j) \text{ with } deg(\phi) = m\}$. This formula comes from the fact that $\{R_i\}$ are endomorphisms of elliptic curves over finite fields, and ideals I_i are isogenies of this form

$$I_i = \{\phi \in Hom(E_z, E_i) \ \forall z \leq n\}$$

using relations from the previous section the equality holds.

Proposition 3.5.10. *For all $m \geq 1$ and $i = 1, ..., n$*

$$t_m e_i = \sum_{j=1}^{n} B_{ij}(m) e_j$$

Proof. Here, we are going to use that $e_i = I_i$. We want to compute the number of points in the divisor class $t_m e_i$ which lie in the $j-$component. To solve this problem we are going to use the analogous definition of the t_m operator for elliptic curves

$$t_m[E_i] = \sum_{j \in \lambda} [E_j]$$

with E_i the elliptic curve associated to the ideal I_i by Deuring's theorem. Now, we have to count the number of isogenies $E_i \to E_j$ of degree m, modulo isogenies with the same kernel. Using the proposition 3.2.4 we have that this number is equal to $B_{ij}(m)$. This gives us the result. ∎

Observation 3.5.11. *On the basis $\{e_i\}$ of $Pic(X)$, the action of t_m is given by $B(m)^{tr}$.*

We define the *height pairing* on $Pic(X)$

$$\langle e_i, e_j \rangle = \begin{cases} 0 & \text{if } i \neq j \\ w_i & \text{if } i = j \end{cases}$$

We can extend this definition to $Pic(X)$ in the natural way. Let $e = \sum a_i e_i$ and $e' = \sum a_i' e_i$, then

$$\langle e, e' \rangle = \sum_{i=1}^{n} w_i a_i a_i'$$

Observation 3.5.12. *This pairing is positive definite and gives an isomorphism of $Pic(X)^\vee = Hom(Pic(X), \mathbb{Z})$ with the subgroup of $Pic(X) \otimes \mathbb{Q}$ with basis $\langle e_i^\vee = e_i/w_i \rangle_{i=1}^n$.*

Proposition 3.5.13. *For all classes e, e' in $Pic(X)$*

$$\langle t_m e, e' \rangle = \langle e, t_m e' \rangle$$

Proof. Since $\{e_1, ..., e_m\}$ is a basis of $Pic(X)$, it suffices to verify the equation with $e = e_i$ and $e' = e_j$. By the previous proposition, we have the explicit behaviour of the t_m operator. Thus we compute

$$\langle t_m e_i, e_j \rangle = w_j B_{ij}(m) \text{ and } \langle e_i, t_m e_k \rangle = w_i B_{ji}$$

by the properties from 3.2.7 both sides are equal. ∎

Those properties of the operator t_m are similar to properties of the Hecke operator T_m. In order to relate these two maps, we are going to obtain some properties about Hecke operators on $M_2(\Gamma_0(N))$.
The set $M_2(\Gamma_0(N))$ is a complex vector space, with $dim(M_2(\Gamma_0(N)) = n$, the *class number.* We can express every function $f \in M_2(\Gamma_0(N))$ as

$$f(\tau) = \sum_{m \geq 0}^{\infty} a_m q^m \text{ with } q = e^{2\pi i \tau}$$

We define a subgroup of this modular forms as

$$M = \left\{ f = \sum_{m \geq 0}^{\infty} a_m q^m \in M_2(\Gamma_0(N)) \text{ s.t } \begin{cases} a_m \in \mathbb{Z} & \text{for all } m \geq 1. \\ W a_0 \in \frac{1}{2}\mathbb{Z} & \text{in other case.} \end{cases} \right\}$$

with $W = \prod_{i=1}^n w_i$. M is a free $\mathbb{Z}-$module of rank n. If we "extend the scalars" $M \otimes \mathbb{C} = M_2(\Gamma_0(N))$. Modular forms $\{f_{ij}\}$ from the previous section are elements of M.
The Hecke algebra $\mathbb{T} = \mathbb{Z}[...T_m...]$, with m prime, acts on M in the following way

$$f|T_m = \begin{cases} \sum_{m \geq 0} a_m q^m | T_p = \sum_{m \geq 0} (a_{mp} + p a_{m/p}) q^m & \text{if } p \neq N \\ \sum_{m \geq 0} a_m q^m | T_N = \sum_{m \geq 0} a_{mN} q^m & \text{with } T_N \end{cases}$$

The subgroup M^+ of M on wich $T_N = 1$ has rank t, the *type number.*

Proposition 3.5.14. *For all $m \geq 1$, we have*

$$f_{ij}|T_m = \sum_k B_{ik}(m) f_{kj} = \sum_k B_{kj}(m) f_{ik}$$

Proof. Since T_m operators with prime m generates $\mathbb{T}$, it suffices to compute $f_{ij}|T_m$, for m prime. Since $f_{ij} = \frac{1}{2w_j} + \sum B_{ij}(m) q^n$, applying this operators we must show

$$B_{ij}(mp) + pB_{ij}(m/p) = \sum_k B_{ik}(p) B_{kj}(m)$$

$$B_{ij}(mN) = \sum_k B_{ik}(N) B_{kj}(m)$$

Those equalities follows by Brandt's matrices properties, 3.2.7. Using the same argument as in the previous proposition, we have the second equality of the statement. ∎

Eichler found a resemblance between Hecke operators over f_{ij} and t_m over $Pic(X)$, given by Brandt matrices. He computed the trace of T_m using the *Lefschetz's fixed point formula*, obtaining that

$$Trace\ T_m = Trace\ B(m)\ \ \forall\, m \geq 1$$

Using this result we can assert that $\mathbb{Z}[...t_m...] \simeq \mathbb{Z}[...T_m...] =$ as $\mathbb{Z}-$modules. From this point on, we are going to see the space M as a $\mathbb{T}-$module. The same will happen with the space $Pic(X)$ in order to relate these two subspaces.
Using the last result we can state that $M \otimes \mathbb{Q} = \langle f_{ij} \rangle$. Moreover, we can find stable subgroups of M using how Hecke operators acts on $\{f_{ij}\}$.

$$\begin{cases} N = & \langle f_{1j}, f_{2j}, ..., f_{nj} \rangle \\ N' = & \langle f_{j1}, f_{j2}, ..., f_{jn} \rangle \end{cases}$$

Proposition 3.5.15. *The following map*

$$\begin{aligned} \phi:\ Pic(X) \otimes_{\mathbb{T}} Pic(X)^{\vee} &\longrightarrow \qquad M \\ \phi(e, e^{\vee}) &\rightarrow \frac{deg\ e \cdot deg\ e^{\vee}}{2} + \sum_{m \geq 1} \langle t_m e, e^{\vee} \rangle q^m \end{aligned}$$

defines a $\mathbb{T}-$module homomorphism, which is an isomorphism over $\mathbb{T} \otimes \mathbb{Q}$.

Proof. First, we need to prove that $\phi(e, e^{\vee}) \in M$. Since the definition of ϕ is based on $\langle \cdot, \cdot \rangle$, ϕ is bi-additive in each variable. This implies that we only need to prove this proposition for $e = e_i$ and $e^{\vee} = e_j^{\vee}$. Using the explicit behaviour of t_m from 3.5.10, we obtain that $\langle t_m e_i, e_j^{\vee} \rangle = B_{ij}(m)$. Using this observation, we obtain that

$$\phi(e_i, e_j^{\vee}) = f_{ij} \in M$$

The $\mathbb{T}-$linearity follows from the fact that t_m and T_m acts on $e_i \in Pic(X)$ and $f_{ij} \in M$ with same expressions (by the Brandt's matrix, 3.5.10 and 3.5.14 respectively)
The surjectivity of this map comes from the fact that with the set $\{e_1, ..., e_n\}$ we can obtain the set $\{f_{ij}\}_{ij}$ via ϕ, and $\{f_{ij}\}_{ij}$ generates M.
Also, $Pic(X) \otimes \mathbb{Q} \simeq Pic(X)^{\vee} \otimes \mathbb{Q}$ and $M \otimes \mathbb{Q}$ are free $\mathbb{T} \otimes \mathbb{Q}-$modules of rank 1. This proves that ϕ defines an isomorphism. ∎

This gives us that $M_2(\Gamma_0(N)) \otimes \mathbb{Q} \simeq Pic(X) \otimes \mathbb{Q}$ as $\mathbb{T}-$modules.

Observation 3.5.16. *This relation gives us a new interpretation of $Pic(X)$. Every element of the Picard group can be seen as a modular form of weight* 2

Observation 3.5.17. *This relation can be seen as an explicit Jacquet-Langlands correspondence. As we said in the previous chapter, the Jacquet-Langlands correspondence is a bijection between some eigenforms of two quaternion algebras. In this case, those two quaternion algebras are $M_2(\mathbb{Q})$, whose eigenforms are cusps forms of weight 2, and B, whose eigenforms are elements of the Picard group.*

We define $e_0 = \sum_{i=1} \frac{1}{w_i} e_i = \sum_{i=1}^{n} e_i^{\vee}$ with $deg(e_0) = \frac{N-1}{12}$. Using the behaviour of t_m given by 3.5.10, we obtain

$$t_m e_0 = \sigma(m)_N e_0$$

For any class $e \in Pic(X)$, we have the following height function

$$\langle e, e_0 \rangle = deg\ e$$

Analyzing the eigenvalues of $M_2(\Gamma_0(N))$, it is known that the only non-cusp form with eigenvalue is the Eisenstein series given by

$$\begin{aligned} F =& \phi(e_i, e_0) \;\; for\ any\ i = 1, ..., n \\ =& \sum_{j=1}^{n} f_{ij} \;\; for\ any\ i = 1, ..., n \\ =& \frac{N-1}{24} + \sum_{m \geq 1} \sigma(m)_N q^m \end{aligned}$$

F satisfies that $F|T_m = \sigma(m)_N F$ for any $m \geq 1$. Since N is a prime number, $S_2(\Gamma_0(N)) = S_2^{new}(\Gamma_0(N))$. This implies that eigenspaces are of dimension 1. Since other eigenvalues are given by $n-1$ cusp form, using the spectral decomposition, we can find a basis of $M_2(\Gamma_0(N))$ such that it includes these cusp forms.
This will allow us to do projections to eigenspaces. We can transfer this property to $Pic(X)$, because $Pic(X) \otimes \mathbb{C} \simeq M_2(\Gamma_0(N))$ as Hecke modules. This obviously implies that if $f = \sum_{m \geq 0} a_m q^m$ is an eigenform associated to c, $t_m c = ac$, and $T_m f = af$ with $a \in \mathbb{C}$. This means that this isomorphism preserve eigenvalues.

3.6 Proof of the main result

To simplify the notation, when we say that we choose $A \in Pic(O)$, we are choosing a representative a of this class.
The proof of this result consists in compute Fourier coefficients of $\sum_{B \in Pic(O)} \phi(x_B, x_{AB})$ for x special point of discriminant $-D$. We will see that this coincides with Fourier coefficients of the Trace. In fact, this computation is based in the arithmetic of optimal embeddings.

Lets B be a quaternion algebra ramified at N and ∞, R it's a fixed maximal order. $K = \mathbb{Q}(\sqrt{-D})$ it's a quadratic field with discriminant $-D$ and x it's a special point with discriminant $-D$. The map ϕ has in its definition the pairing $\langle x_B, t_m x_{AB} \rangle$. In order to compute this, we must determine in $M(R)$ in how many coordinates coincides $t_m x_{AB}$ and x_B.
Since the components of X are indexed by supersingular elliptic curves in characteristic N, we can rewrite this pairing as an elliptic curve problem

$$\langle x_B, t_m x_{AB} \rangle = \frac{1}{2}[\phi \in Hom(E, E')\ s.t\ deg\ \phi = m]$$

with E and E' elliptic curves associated to each component of x_A and x_{AB}. We are going to denote $Hom(E, E')$ by $Hom(x_B, x_{AB})$.

By the definition of the curve X, if we have a point x of discrminant $-D$, we also have a homomorphism $f:\ K \hookrightarrow B$, this means that we can rewrite the algebra B as $f(K) + f(K)j$.

Proposition 3.6.1. *If we have an embedding $f:\ K \hookrightarrow B$, we can rewrite the algebra as*

$$B = K + Kj$$

with $j^2 = -N$ and $j\alpha = \overline{\alpha} j$ for all $\alpha \in K$.

Observation 3.6.2. *Due to the last proposition, lets $x = g \times y$. If we rewrite the algebra B in terms of x, we can identify y with the inclusion i*

$$\begin{aligned} i:\ K \hookrightarrow& K + Kj \\ \alpha \rightarrow& \alpha \end{aligned}$$

Lets O be the ring of integers of K, $\mathfrak{D} = (\sqrt{-D})$ the different ideal of O. Lets $\epsilon^2 = -N\ (D)$, which existence is given by the last proposition. A student of Gross proved that there exists an elliptic curve E such that its endomorphism ring is of the following form

$$End(E) = \{\alpha + \beta j \ s.t\ \alpha \in \mathfrak{D}^{-1},\ \beta \in \mathfrak{D}^{-1},\ \alpha \equiv \epsilon\beta\ (mod\ O)\}$$

We can identify this elliptic curve with a point of X. Since supersingular elliptic curves are 1-1 identified with orders of a quaternion algebra, there exists a special point of discriminant $-D$, x, associated to E. By this relation, if the point is $x = g \times y$ then $O_R(\hat{R}g \cap B) = End(E)$. From now on, we are going to denote $End(E)$ by $End(x)$.

Observation 3.6.3. *$End(x)$ is a maximal order because is the Endomorphism ring of a supersingular elliptic curve.*

From now on, we denote by x the point of discrmininant $-D$ such that $O_R(\hat{R}g \cap B) = End(E)$, with $End(E)$ as we defined before.
We are going to compute explicitly an expression for $Hom(x_B, x_{BA})$. In order to do this, we will need three auxiliary lemmas.

Lemma 3.6.4. *Lets $b \in B$ be an ideal class of O. The next equality holds*

$$O_R(x_A) = O_R(End(x)B)$$

Proof. Let $\alpha \in O_R(x_B)$, given $u \in End(x)b$, we are going to prove that $u\alpha \in End(x)b$. Once we have proved it, we will have the inclusion $O_R(x_B) \subseteq O_R(End(x)b)$. Since both orders are maximal, this gives the equality between the sets.
Now, to prove the inclusion, lets $u \in End(x)b$. We can express $u = \sum h_i b_i$ where $h_i \in End(x)$ and $b_i \in b$. As we know, $End(x) = O_R(I)$ for some ideal I. This verifies that $Ih_i \subset I$ and $b_i \in b$. With this observation, to prove that $u\alpha \in End(x)b$, is enough to prove that

$$Iu\alpha \subset Ib$$

this follows from

$$Iu\alpha = I(\sum_i b_i)\alpha \subset Ib\alpha \subset Ib$$

∎

Lemma 3.6.5. *Lets $a, b \in A, B \in Pic(O)$, then*

$$Hom(x_B, x_{BA}) = O_R(x_B)A$$

Proof. Until now, the definition of $Hom(x_B, x_{BA})$ has been in terms of elliptic curves. We have a $1-1$ correspondence between those curves and orders. We can rewrite $Hom(x_B, x_{BA})$ using orders by the theory of the previous chapter

$$Hom(x_B, x_{BA}) = \{\alpha \in B^* \ s.t\ gb\alpha \subset gba\}$$

where we have used that $x = g \times y$, and we can suppose that $y = i$ is the inclusion by 3.6.1.
Also, we have that $gbO_R(x_B)a = gb$, concluding with

$$gb\alpha \subset gba = gBO_R(x_B)A \Longleftrightarrow \alpha \in O_R(x_B)a$$

∎

Lemma 3.6.6. *Lets $B \in Pic(O)$, $b \in B$, then $End(x)B$ is a left ideal of $End(x)$ and verifies that*

$$End(x)B = \{\gamma + \delta j \ s.t\ \gamma \in \mathfrak{D}^{-1}b,\ \delta \in \mathfrak{D}^{-1}\overline{b},\ \gamma \equiv \epsilon\delta\ (mod\ O)\}$$

Proof. Lets $\alpha+\beta j \in L$, any $b \in B$ has the expression $b = m + n\sqrt{-D}$. Multiplying we have that

$$(\alpha+\beta j)b = \alpha b + \beta j b = \alpha b + \beta \overline{b} j \in \mathfrak{D}^{-1}b + \mathfrak{D}^{-1}\overline{b}j$$

These elements verifies the congruence $\alpha b = \epsilon\beta\overline{b}\ (mod\ O)$, since

$$\alpha b - \epsilon\beta\overline{b} = \alpha b - \epsilon\beta(b - 2n\sqrt{-D}) = (\alpha-\epsilon\beta)b - 2n\beta\sqrt{-D} \in O$$

where we have used that $\beta\sqrt{-D} \in \mathfrak{D}^{-1}\mathfrak{D} = O$. The equality follows because $\mathfrak{D}$ is the different ideal of O.
This proves the inclusion

$$Lb \subset \{\gamma+\delta j:\ \gamma\in\mathfrak{D}^{-1}b,\ \delta\in\mathfrak{D}^{-1}\overline{b},\ \gamma\equiv\epsilon\delta\ (mod\ O)\}$$

To prove the other inclusion, lets $y = \gamma+\delta j$ with $\gamma \in \mathfrak{D}^{-1}b$ and $\delta = \frac{\overline{b}}{\sqrt{-D}} \in \mathfrak{D}^{-1}\overline{b}$. Since $b \in B$, $\overline{b} = m - n\sqrt{-D}$ with $m, n \in \mathbb{Z}$. This satisfies the condition $\gamma \equiv \epsilon\delta\ (mod\ O)$. Then, there exist $\lambda \in O$ such that $\gamma = \epsilon\delta + \lambda$ and

$$y = \lambda + \epsilon\delta + \delta j = \delta + \epsilon\frac{b - 2n\sqrt{-D}}{\sqrt{-D}} + \frac{\overline{b}}{\sqrt{-D}}j = \lambda - 2n\epsilon + (\frac{\epsilon}{\sqrt{-D}} + \frac{1}{\sqrt{-D}}j)b \in Lb$$

∎

Theorem 3.6.7. *Lets $b \in B \in Pic(O)$ and $a \in A \in Pic(O)$*

$$Hom(x_b, x_{ba}) = \{\alpha+\beta j\ s.t\ \alpha\in\mathfrak{D}^{-1}a,\ \beta\in\mathfrak{D}^{-1}b^{-1}\overline{b}\overline{a},\ \alpha\equiv\epsilon\beta\ (mod\ O)\}$$

Proof. Using the previous three lemmas, it is enough to prove that

$$O_R(\{\gamma+\delta j\ s.t\ \gamma\in\mathfrak{D}^{-1}b,\ \delta\in\mathfrak{D}^{-1}\overline{b},\ \gamma\equiv\epsilon\delta\ (mod\ O)\})a =$$
$$\{\alpha+\beta j\ s.t\ \alpha\in\mathfrak{D}^{-1}a,\ \beta\in\mathfrak{D}^{-1}b^{-1}\overline{b}a,\ \alpha\equiv\epsilon\beta\ (mod\ O)\}$$

Lets

$$J = \{\gamma+\delta j\ s.t\ \gamma\in\mathfrak{D}^{-1}b,\ \delta\in\mathfrak{D}^{-1}\overline{b},\ \gamma\equiv\epsilon\delta\ (mod\ O)\}$$
$$L = \{\alpha+\beta j\ s.t\ \alpha\in\mathfrak{D}^{-1},\ \beta\in\mathfrak{D}^{-1}b^{-1}\overline{b},\ \alpha\equiv\epsilon\beta\ (mod\ O)\}$$

We are going to prove that $O_R(J) = L$ and then, $Hom(x_b, x_{ba}) = La$.
Lets $h = \gamma+\delta j \in J$ and $b = \alpha+\beta j \in L$, multiplying we have that

$$\begin{cases} \gamma\alpha - N\delta\overline{\beta} \in \mathfrak{D}^{-1}b \\ \delta\overline{\alpha} + \gamma\beta \in \mathfrak{D}^{-1}\overline{b} \\ \gamma\alpha - N\delta\overline{\beta} \equiv \epsilon(\delta\overline{\alpha}+\gamma\beta)\ (mod\ O) \end{cases}$$

∎

This theorem gives us an explicit definition of elements of $Hom(x_B, x_{BA})$. We have that $\langle x_B, t_m(x_{BA})\rangle = \frac{1}{2}\#\{f \in Hom(x_B, x_{BA})\ s.t\ deg(f) = m\}$. If we combine the restriction on the degree with the previous theorem, we have that $\alpha+\beta j \in Hom(x_B, x_{BA})$ must obey the following condition

$$\mathfrak{N}(\alpha) + N\mathfrak{N}(\beta) = m\mathfrak{N}(a)$$

Now, we have to compute the cardinality of the pairs (α, β) with $\alpha \in \mathfrak{D}^{-1}a$, $\beta \in \mathfrak{D}^{-1}b^{-1}\overline{b}\overline{a}$ and $\alpha \equiv \epsilon\beta\ (mod\ O)$. We can rewrite this equation in the following way

$$\begin{aligned} \mathfrak{L} &= (\alpha)\mathfrak{D}a^{-1} \in A^{-1} \\ \mathfrak{L}' &= (\beta)\mathfrak{D}b^{-1}\overline{b}^{-1}\overline{a}^{-1} \in AB^2 \\ \mathfrak{N}(\mathfrak{L}) + N\mathfrak{N}(\mathfrak{L}') &= mD \end{aligned}$$

Now we have an ideal equation, this benefits us, because we can express the number of solutions to this equation using modular forms $E_{A^{-1}}(z)$ and $E_{AB^2}(z)$.

Proposition 3.6.8. *Lets N, D be prime numbers*

$$\sum_{B\in Pic(O)} \langle x_B, t_m(x_A B)\rangle = u^2 \sum_{n=0}^{mD/N} r_A(mD-nN)\delta(n)R(n)$$

where $\delta(n) = \begin{cases} 1 & \text{if } (n,D)=1 \\ 2 & \text{if } d\equiv 0 \ (mod\ D) \end{cases}$

Proof. First, we count the number of ideals $\mathfrak{L}$ and $\mathfrak{L}'$ by

$$r_{A^{-1}}(mD) + \sum_{n>0} r_{A^{-1}}(mD-nN) r_{AB^2}(n)$$

where $n = \mathfrak{N}(\mathfrak{L}')$ and $mD - nN = \mathfrak{N}(\mathfrak{L})$. A solution to this ideal equation gives a solution to our main equation (The main equation is in term of elements).
If we set a solution $\mathfrak{L}$ and $\mathfrak{L}'$, using that there are w unities, we have a priori w^2 possible choices for α, β, except when $n=0$, when there are w choices. Of all those options, when $n\equiv 0\ (D)$ every element satisfies the condition $\alpha \equiv \epsilon\beta\ (mod\ O)$. When $n \neq 0\ (mod\ D)$, only half of them satisfies this requirement. Then, we conclude with

$$\langle x_B, t_m x_{AB}\rangle = u^2 \sum_{n=0}^{mD/N} r_{A^{-1}}(mD-nN)\delta(n) r_{AB^2}(n)$$

If we sum this over all classes B and we use that $\sum r_{AB^2}(n) = R(n)$, we obtain the statement. We have used that as D is prime and there are no elements of order 2 in $Pic(O)$. ∎

Now we can compare the trace computation with this expression. We have proved that

$$\sum_{B\in Pic(O)} \langle x_B, t_m(x_{AB})\rangle = u^2 a_m \textit{ for all } m\geq 1$$

Using this observation we can conclude with

Corollary 3.6.9. $u^2 G_A = \sum_{B\in Pic(O)} \phi(x_B, x_{AB})$ *in M. We can rewrite the $L-$function as*

$$L(f,A,1) = \frac{(f,G_A)}{\sqrt{D}}$$

3.7 Variations of the $L-$function

Along this subsection, we are going to define other $L-$functions related to the previous one. We will compute their special values in a similar way of how we did before. The idea behind this result is that we can "project" special points of the Shimura curve X by certain operators, as we saw in the previous theory.

Lets χ be a character such that $\chi:\ Pic(O)\to\mathbb{C}$. Lets f be a normalized eigenform for the Hecke algebra $\mathbb{T}$, we define

$$L(f,\chi,s) = \sum_{A\in Pic(O)} \chi(A) L(f,A,s)$$

To describe values of $L(f,\chi,1)$ at $s=1$, we are going to use the projection of divisors $x_\chi = \sum_{A\in Pic(O)} \chi^{-1}(A) x_A$. As we said in the previous subsection, we can obtain the projection of c_χ associated to f, $c_{f,\chi}\in Pic(X)\otimes\mathbb{C}$. Using that f is a cusp form we can deduce that $deg\ c_{f,\chi} = 0$.

Proposition 3.7.1. $L(f,\chi,1) = \frac{(f,f)}{u^2\sqrt{D}}\langle c_{f,\chi}, c_{f,\chi}\rangle$

Proof. We can extend the $\mathbb{R}-$bilinear pairings $\langle\cdot,\cdot\rangle$ and $\phi(\cdot,\cdot)$ to complex pairings which are linear in the first argument and anti-linear in the second. We compute

$$\langle c_\chi, c_\chi\rangle = \langle\sum_A \chi^{-1}(A)x_A, \sum_B \chi^{-1}(B)x_B\rangle = \sum_{A,B}\chi(A^{-1}B)\langle x_A, x_B\rangle$$

Combining this result with the main definition, we can state that

$$L(f,\chi,1) = \frac{(f,\sum_A \chi(A)g_A)}{u^2\sqrt{D}}$$

Now we have to prove that the coefficient of f in the eigenvector expansion of $\sum\chi(A)g_A$ is equal to $\langle c_{f,\chi}, c_{f,\chi}\rangle$

$$\sum\chi(A)g_A = \sum_A\chi(A)\sum_B\phi(x_B, x_{AB}) = \sum_{A,B}\chi(A)\phi(x_B, x_{AB})$$

doing a variable change such that $A' = B$ and $B' = AB$, we have that

$$\sum_{A,B}\chi(A)\phi(x_B,x_{AB}) = \sum_{A',B'}\chi(A'^{-1}B')\phi(x_{A'},x_{B'}) = \phi(c_\chi, c_\chi)$$

Now we are going to use the fact that we can do projections. The map ϕ is $\mathbb{T}-$bilinear, then the $f-$eigencomponent of the modular form $\phi(c_\chi, c_\chi)$ is equal to

$$\phi(c_{\chi,f}, c_\chi) = \phi(c_{\chi,f}, c_{\chi,f}) = \sum_{m\geq 1}\langle c_{\chi,f}, t_m c_{\chi,f}\rangle q^m$$

where we have used that if π is a projection, then $\pi(\pi(a)) = \pi(a)$.

$$\sum_{m\geq 1}\langle c_{\chi,f}, t_m c_{\chi,f}\rangle q^m = \sum_{m\geq 1}\langle c_{\chi,f}, c_{\chi,f}\rangle a_m(f) q^m = \langle c_{\chi,f}, c_{\chi,f}\rangle f$$

In the last equality we have used that t_m preserves the eigenvalues. ∎

Corollary 3.7.2. *1. $L(f,\chi,1)\geq 0$, and we obtain the equality if and only if $c_{f,\chi} = 0$.*

2. For any automorphism α of $\mathbb{C}$, we have the following result

$$(L(f,\chi,1)\sqrt{D}/(f,f))^\alpha = L(f^\alpha,\chi^\alpha,1)\sqrt{D}/(f^\alpha,f^\alpha)$$

3. $L(f,\chi,1) = 0$ if and only if $L(f^\alpha,\chi^\alpha,1) = 0$

Proof. 1. By 3.7.1, we have that $L(f,\chi,1) = \frac{(f,f)}{u^2\sqrt{D}}\langle c_{f,\chi}, c_{f,\chi}\rangle$. Now, we only have to check the sign of $\langle c_{f,\chi}, c_{f,\chi}\rangle$. This pairing induces a positive definite Hermitian pairing on $Pic(X)\otimes\mathbb{C}$. This gives the result.

2. We have that $\langle\cdot,\cdot\rangle$ is a rational pairing on $Pic(X)\otimes\mathbb{Q}$, then

$$\langle c_{f,\chi}, c_{f,\chi}\rangle^\alpha = \langle c_{f^\alpha,\chi^\alpha}, c_{f^\alpha,\chi^\alpha}\rangle$$

3. Follows by the previous result.

∎

If we fix the character $\chi = 1$, we obtain other $L-$function that has a large importance in number theory. This is the $L-$function of an elliptic curve. We have the following decomposition

$$L(f,\chi = 1,1) = L(f,1)L(f\otimes\epsilon,1)$$

where $f \otimes \epsilon = \sum_{m \geq 1} a_m \epsilon(m) q^m$, this is named *the twist of f*. This new modular form has level ND^2.
To obtain information about the function, we have to define some objects. Let c_D be a rational divisor of X with the following definition

$$c_D = \frac{1}{2} \sum_{-D=df^2} \frac{1}{u(d)} \sum_{\substack{x \text{ special point} \\ \text{of disc } d \text{ on } X}} (x)$$

Using the theory from the last section, we obtain that $deg(c_D) = H_N(D)$. Now we can obtain the class of this divisor, e_D, that lies in $Pic(X) \otimes \mathbb{Q}$.

Proposition 3.7.3. *The class* e_D *lies in the subgroup* $Pic(X)^\vee$ *of* $Pic(X) \otimes \mathbb{Q}$.

Proof.

$$e_D = \sum_{i=1}^{n} (\sum_{-D=df^2} \frac{h_i(d)}{2u(d)}) e_i = \sum_{i=1} (\sum_{-D=df^2} \frac{w_i h_i(d)}{2u(d)}) e_i^\vee$$

Now, we must show that

$$\frac{w_i h_i(d)}{2u(d)} \in \mathbb{Z}$$

If w_i is odd, then $u(d)|w_i$ and 2 divides $h_i(d)$. If $w_i \equiv 2 \ (mod\ 4)$ the only problem comes up when $u(d) = 2$. Using the theory of quadratic fields, we can see that in this case $d = -4$, N is odd and $h_i(d)$ is even. ∎

Using the explicit definition of e_D as we used in the previous proposition, we can rewrite c_χ as

$$c_\chi = \sum_{A \in Pic(O)} x_A \equiv u e_D$$

where we have applied that $Pic(O) \times Gal(K/\mathbb{Q})$ acts simply transitively on special points. It is important to remark that components of X are stable under the Galois action.

Corollary 3.7.4. $L(f,1)L(f \otimes \epsilon_D, 1) = \frac{(f,f)}{\sqrt{D}} \langle e_{f,D}, e_{f,D} \rangle$.

Proof. Substituting $c_\chi = \sum_{A \in Pic(O)} x_A \equiv u e_D$ in proposition 3.7.1. ∎

3.8 Reinterpretation using modular forms of weight 3/2

The relation between modular forms of weight even and modular forms of half integer weight comes from a Shimura research. He states the following results for modular forms of half weight

1. The level of the forms is always a number N divisible by 4.
2. There are Hecke operators $T^*_{n^2}$, $\forall n \in \mathbb{N}$ with $(n, N) = 1$.
3. Let $f \in S_{k+1/2}(\Gamma_0(N))$, we have some liftings which send f to a certain $f' \in S_{2k}(\Gamma_0(N/2))$. These liftings conmute with the action of Hecke operators.

As we have been using modular forms of weight 2 along the previous subsections, we are going to consider modular forms of weight 3/2 with level $4N$, i.e, $M_{3/2}(\Gamma_0(4N))$. We are going to use that a modular form $g \in M_{3/2}(\Gamma_0(4N))$ has the following property

$$g(\tau)/\theta(\tau)^3 \text{ is invariant under } \Gamma_0(4N)$$

where $\theta(\tau) = \sum q^{n^2}$ is the standard theta-serie of weight 1/2.
We denote the Fourier expansion of g as

$$g(\tau) = \sum_{D\geq 0} a_D q^D$$

We can define a subspace of $M_{3/2}(\Gamma_0(N))$ called *Kohnen's subspace*. We are going to denote it by $M^*_{\mathbb{C}}$.

$$M^*_{\mathbb{C}} = \{g = \sum_{D\geq 0} a_D q^D \in M_{3/2}(\Gamma_0(N)) \ s.t \ a_D = 0 \ unless \ -D \equiv 0,1 \ (mod\ 4) \ and \ (\frac{-D}{N}) \neq 1\}$$

Kohnen's subspace has dimension t, the *type number*, and it is stable under Shimura operators $T^*_{n^2}$. Kohnen also defined operators T_{m^2} on $M^*_{\mathbb{C}}$ for all m. He used the trace formula to prove that

$$Trace\ T^*_{m^2} = Trace\ T_m|M_2(\Gamma_0(N))^+$$

where $M_2(\Gamma_0(N))^+$ is the subspace of $M_2(\Gamma_0(N))$ with $T_N|_{M_2(\Gamma_0(N))^+} = 1$.
We describe the explicit action of the operators $T_{n^2}*$ for a prime n as

$$\begin{cases} \sum_{D\geq 0} a_D q^D | T^*_{p^2} = \sum_{D\geq 0} (a_{Dp^2} + (\frac{-D}{N}) a_D + p a_{D/p^2}) q^D & \text{if } p \neq N \\ \sum_{D\geq 0} a_D q^D | T^*_{N^2} = \sum_{D\geq 0} a_{DN^2} q^D \end{cases}$$

On the Kohnen subspace, the operators acts by the identity, i.e $a_D = a_{DN^2}$. Also, we are going to consider a lattice M^* over the Kohnen subspace.

$$M^* = \left\{ f = \sum_{D\geq 0} a_D q^D \in M^*_{\mathbb{C}} \ s.t \begin{cases} a_D \in \mathbb{Z} & \text{if } D > 0 \\ a_0 \in \frac{1}{2}\mathbb{Z} \end{cases} \right\}$$

This lattice has rank t and it is stable under the Hecke algebra $\mathbb{T}^*$. Now we are going to construct some elements of M^* using the theory about quaternion algebras. This functions will allow us to describe special values of $L(f,1)L(f\otimes\epsilon,1)$.

For each i with $1 \leq i \leq n$ let S_i the suborder of index 8 in R_i defined as

$$S_i = \mathbb{Z} \oplus 2R_i$$

We denote by S_i^0 to the subgroup of S_i with trace zero. This subgroup has rank 3 over $\mathbb{Z}$. We associate to each lattice S_i the theta-serie g_i as follows

$$g_i(\tau) = \frac{1}{2}\sum_{b\in S_i^0} q^{\mathfrak{N}(b)} = \frac{1}{2} + \sum_{D>0} a_i(D) q^D$$

We can deduce that the coefficients $a_i(D)$ are one half of the number of $b \in R_i$ such that

$$\begin{cases} b & \equiv 0,1 \ mod\ 2R_i \\ Tr\ b & = 0 \\ \mathfrak{N}(b) & = D = -b^2 \end{cases}$$

Every coefficient $a_i(D)$ is an integer, using reciprocity law, we can observe that $a_i(D)$ is zero unless $-D \equiv 0,1\ (mod\ 4)$ and $(\frac{-D}{N}) \neq 1$. There exists a result which states that $g_i(\tau)$ are modular forms of weight 3/2 and level $4N$. We conclude with that $g_i \in M^*$.

Using the relation between orders and elliptic curves, if we have two orders R_i and R_j which have associated elliptic curves E_i and E_i^N, then orders are conjugated in B. This informs us that both orders generates the same theta-series. As there are only t distinct orders, we conclude that there are t distinct g_i modular forms.

Proposition 3.8.1. *For $1 \leq i \leq n$ and $D > 0$, we have*

$$a_i(D) = \frac{w_i}{2} \sum_{-D=df^2} \frac{h_i(d)}{u(d)}$$

where $h_i(d)$ is the number of optimal embeddings of the order of discriminant d into R_i, modulo conjugation by R_i^*.

Proof. Lets O be the order of discriminant $-D$, then any embedding $f : O \hookrightarrow R_i$ gives us an element $b = f(\sqrt{-D})$ with trace 0 and norm D. Using that $O = \mathbb{Z} \oplus \mathbb{Z}(\frac{D+\sqrt{-D}}{2})$, we have the congruence $b \equiv -D \ (mod\ 2R_i)$. Then $b \in S_i^0$ and contributes to $c_i(D)$.
Conversely, given $b \in S_i^0$ we have that $b^2 = -D$ and then $b \equiv -D \ (mod\ 2R_i)$. We use that $\frac{b+D}{2} \in R_i$ obtaining the embedding $f : O \hookrightarrow R_i$ such that $\frac{\sqrt{-D}+D}{2} \xrightarrow{f} \frac{b+D}{2}$. With w_i the proof is completed. When $w_i > 1$, then we takes Γ_i orbits and analyse the stabilizers. ∎

Proposition 3.8.2. *For all $m \geq 1$ we have*

$$g_i | T^*_{m^2} = \sum_k B_{ik}(m) g_k = w_i \sum_k B_{ki}(m)(g_k/w_k)$$

Subgroups $\langle g_1, .., g_n\rangle$ and $\langle g_1/w_1, ..., g_n/w_n\rangle$ are stable under the Hecke algebra $\mathbb{T}^*$, and T_{m^2} acts on this sets by $B(m)^{tr}$ and $B(m)$ respectively.

Proof. First, we can observe that since the $\mathbb{Z}-$algebra $\mathbb{T}^*$ has the same trace as $\mathbb{T}$, then it suffices to check this statement for m prime. We are going to divide the proof in two steps; for $m = N$ and for $m \neq N$.
When $m = N$, we have to understand the sum $\sum_k B_{ik}(N) g_k$. As we saw in the last section at 3.2.7, $\sum_k B_{ik}(N) = 1$ and $B_{ik}(N) = 1$ if and only if the elliptic curves E_i and E_j are conjugated by automorphism. As we know, the elliptic curve E_i has associated an order R_i by its endomorphism ring. Then, in the sum $\sum_k B_{ik}(N) g_k$, $B_{ik}(N) = 1$ when $g_k = g_i$, since their orders are the same. Then, we have that

$$\sum_k B_{ik}(N) g_k = g_j \ \textit{such that}\ g_j = g_i$$

Furthermore, we can compute $g_i|T^*_{m^2}$ using the explicit result

$$g_i|T^*_{N^2} = \frac{1}{2} + \sum_i a_i(DN^2) q^D$$

using 3.8.1, $a_i(DN^2) = a_i(D)$ since $h_i(DN^2) = 0$ (we know that $h_i(DN^2) = 0$ because we have that $\sum_i h_i(DN^2) = 0$ by the formula given in the proof of 3.1.3). Then, since both sides are equal, we have the equality.

When $m \neq N$, using the explicit result for the $T^*_{m^2}$ operators, we have to chech that

$$a_i(Dp^2) = (\frac{-D}{p}) a_i(D) + p a_i(D/p^2) = \sum_k B_{ik}(p) a_k(D)$$

First, we are going to assume that $D \not\equiv 0 \ (mod\ p)$, then we have that $a_i(D/p^2) = 0$.
We need to understand what means $\sum_k B_{ik}(p) a_k(D)$. On one hand, we have that $B_{ik}(p) = \#\{\phi \in Hom(E_i, E_k) \ s.t\ deg(\phi) = p\}$. On the other hand $a_k(D) = \#\{a \in S_k^0 \ s.t\ \mathfrak{N}(a) = D\}$. Then, we can see this product of cardinals, as the cardinal of the set of elements of the following form

$$\phi^\vee \circ a \circ \phi \ \textit{with}\ \phi\ \textit{and}\ a\ \textit{as before}$$

Since $\phi\ E_i \to E_k$ then $\phi^\vee : E_k \to E_i$. Also $a \in S_k^0$, this means that we can see a as $a \in End(E_k)$. As we have seen, we can transfer operations from the quaternion algebra to isogenies. In this case,

the norm of $b = \phi^\vee \circ a \circ \phi$ is Dp^2 and the trace is zero.
In fact, all elements b with this trace and this norm which are not divisible by p in S_i are obtained uniquely as $\phi^\vee \circ a \circ \phi$. Then, we have to count elements of this norm. This cardinal is given by $a_i(Dp^2)$. We have a restriction given by the fact that $(\phi^\vee)^\vee = \phi$. This will create a pathology in our counting:
Lets $\phi: E_i \to E_k$ be the unique isogeny of degree p such that $ker\ \phi \subset ker\ b$. Then we have that the isogeny factors through $E_i \xrightarrow{\phi} E_k \xrightarrow{\psi} E_i$ for some ψ. Since $b + b^\vee = 0$, $ker\ \phi$ is the unique subgroup of order p in $ker\ b^\vee$. Hence $ker\ \phi \subset ker\ \psi^\vee$ and the dual diagram factors as

$$\begin{tikzcd} E_i & E_i \arrow[l, "b^\vee"'] \arrow[d, "\phi"] \\ E_k \arrow[u, "\phi^\vee"] & E_k \arrow[l, "a^\vee"] \end{tikzcd}$$

This diagram defines $a^\vee$, and hence $a \in S_k$. This means that we have to substract $a_i(D)$ elements to $a_i(Dp^2)$ in our count.

Now we have to count elements b divisible by p in S_i. An element b is divisible by p in S_i if a stabilizes the subgroup $\phi(E_i[p]) = ker\ \phi^\vee$. There are $(1 + (\frac{-D}{p}))$ subgroups of this type, and then, there are the same number of isogenies with this property. Each one gives us a way to write $b = \phi^\vee \circ a \circ \phi$. Hence we can write

$$\sum_k B_{ik}(p)a_k(D) = (a_i(Dp^2) - a_i(D)) + (1 + (\frac{-D}{p}))a_i(D) = a_i(Dp^2) + (\frac{-D}{p})a_i(D)$$

The case with $p|D$ is analogous.
The second equality at the statement follows from the first, as $w_k B_{ik}(m) = w_i B_{ki}(m)$. ∎

We define the following function

$$G = \sum_{i=1}^{n} \frac{1}{w_i} g_i$$

Using the explicit definition of Fourier coefficients from 3.8.1 and also applying the Eichler's formula, we have that G has the following Fourier expansion

$$G = \frac{N-1}{24} + \sum_{D>0} H_N(D)q^D$$

Using how the operators T_{m^2} acts on g_i and the properties of Brandt's matrices, we see that G is an eigenvector for $\mathbb{T}^*$ with eigenvalues $\sigma(m)_N$, i.e

$$G|T^*_{m^2} = \sigma(m)_N G \textit{ for all } m \geq 1$$

Now, as the weight of this modular forms is multiplicative and θ has wieght $1/2$, we can apply T_4 to $G\theta$

$$G\theta|T_4 = \sum_{i=1}^{n} f_{ii}$$

where we have used the Eichler's trace formula. We can observe that T_4 takes $G\theta$ to a form of level N, which generates $M \otimes \mathbb{Q}$ over $\mathbb{T} \otimes \mathbb{Q}$.

3.9 Waldspurger's formula

Using $e_D \in Pic(X)^\vee$ and the $e_0 = \sum_{i=1}^n e_i^\vee$, we define

$$g = \frac{1}{2}e_0 + \sum_{D>1} e_D q^D$$

This is a formal series, but it can be seen as a modular form of weight 3/2 with coefficients on $Pic(X)^\vee$, i.e, elements of $Pic(X)^\vee \otimes M^*$. Using proposition 3.8.1, we can rewrite the serie as

$$g = \sum_{i=1}^{n} e_i^\vee \otimes g_i$$

with g_i the theta-series defined in the previous subsection and $e_i^\vee = e_i/w_i$, the basis of $Pic(X)^\vee$.

Proposition 3.9.1. *g is an element of $Pic(X)^\vee \otimes_{\mathbb{T}} M^* = Hom_{\mathbb{T}}(Pic(X), M^*)$, and for every class $e \in Pic(X)$, the series*

$$g(e) = \frac{deg\ e}{2} + \sum_{D>1} \langle e, e_D\rangle q^D$$

are elements of M^*, and they respect operators, i.e, $g(t_m e) = g(e)|T^*_{m^2}$ for all $m \geq 1$.

Proof. Since $\langle e_1, ..., e_n\rangle$ generates $Pic(X)$, then it suffices to check that $g(e_i) \in M^*$. This follows by the fact that $g(e_i) = g_i \in M^*$.
The second part of the statement follows by 3.5.10, that gives us that $g(t_m e_i) = \sum_{j=1}^n B_{ij}(m) g_i$. Furthermore, proposition 3.8.2 tells us that $g_i|T^*_m = \sum_{j=1}^n B_{ij}(m) g_i$, this gives the equality. ∎

As the number N is prime, the space $M_2(\Gamma_0(N))$ are all newforms. This means that we can obtain a basis of eigenvectors with eigenspaces of dimension 1. Let e_f be a non-zero element in the $f-$isotypical component of $Pic(X) \otimes \mathbb{R}$ (with f eigenform for $\mathbb{T}$). The element e_f is determined up to real scalar multiple. We can define the modular form

$$g(e_f) = \sum_{D \geq 0} m_D q^D$$

that lies in the $f-$isotypical component of $M^* \otimes \mathbb{R}$. It is zero unless $f|T_N = f$.

Proposition 3.9.2. *Let $-D$ be a fundamental discriminant with $(\frac{-D}{N})$, then*

$$L(f,1)L(f \otimes \epsilon, 1) = \frac{(f,f)}{\sqrt{D}} \frac{m_D^2}{\langle e_f, e_f\rangle}$$

Proof. We are going to obtain the result using 3.7.4. If we prove that $\langle e_{f,D}, e_{f,D}\rangle = \frac{m_D}{\langle e_f, e_f\rangle}$, then we will have the equality.
By definition, we have that $m_D = \langle e_f, e_D\rangle = \langle e_f, e_{f,D}\rangle$. Hence as the definition of $\langle\cdot,\cdot\rangle$ is defined by the coordinates where e_f and $e_{f,D}$ coincides and both elements are in the same coordinate, we have that

$$e_{f,D} = \frac{m_D^2}{\langle e_f, e_f\rangle} e_f \ \textit{in}\ (Pic(X) \otimes \mathbb{R})^f$$

∎

Corollary 3.9.3. *The rank of the subgroup $\langle g_1, ..., g_t\rangle$ is equal to the number of eigenforms f, including Eisenstein series of weight 2, with $L(f,1) \neq 0$.*

Proof. Since $g = \sum_{i=1}^n e_i^\vee \otimes g_i$, to obtain the rank of $\langle g_1, ..., g_t\rangle$ it suffices to determine which eigenforms f satisfy $g(e_f) \neq 0$. By the previous proposition, as the formula

$$L(f,1)L(f \otimes \epsilon, 1) = \frac{(f,f)}{\sqrt{D}} \frac{m_D^2}{\langle e_f, e_f\rangle}$$

uses the coefficients of $g(e_f)$, then $g(e_f) \neq 0$ if $L(f,1)L(f \otimes \epsilon_D, 1) \neq 0$ for a fundamental discriminant $-D$, such that $(\frac{-D}{N}) = 1$. Waldspurger show that it is always possible to obtain a D such that $(\frac{-D}{N}) = -1$ and $L(f \otimes \epsilon_D, 1) \neq 0$. We reduce this result to $L(f,1) \neq 0$. ∎

3.10 Gross-Zagier formulae from a higher point of view

In this section we are going to show a more general point of view of the Gross-Zagier formulae. Along this chapter, we have been focusing on solving the formula for the $L-$function, but we can define this theory in a bigger area of number theory. We can relate all the theory of $L-$functions with Galois representations, allowing us to translate problems from the modular world to the representation theory world. The aim of this section is to explain what is the general point of view of the Gross formula and to give some results about this theory, giving the general idea of how the Peterson product works, what is the theta function defined and some properties of it. This section was thought as an ending section, where we give general ideas about the context where this dissertation can be seen. We will not give proofs or detailed explanations, just an abstract of what are the following steps on this theory. This section gives a more general point of view of why this formula arises and how Gross could reach this result.

We start this section giving the definition of $L-$function via Galois representation, a powerful definition that allows us to see all this theory from other point of view. We can define $L-$functions in terms of Galois representations as

Definition 3.10.1. *Let k be a topological field. Let K be a number field and*

$$\rho: \; G_K \to GL_n(k)$$

a global Galois representation. Suppose that its characeristic polynomial of Frobenius

$$\widetilde{\Phi}(\rho)(X) = det(1 - XFrob_{K_p}|V^{I_{K_p}}) \in \overline{Q}[X]$$

We define the partial $L-$function of ρ as

$$\mathcal{L}(\rho, s) = \prod_{\mathfrak{p} \; unramified} \frac{1}{\widetilde{\Phi}_{\mathfrak{p}}(\rho)(N(\mathfrak{p})^{-s})}$$

This definition coincides with the classical definitions of $L-$functions due to the next definitions

Definition 3.10.2. *Let K be a field and A an abelian variety of dimension g over K. The absolute Galois group G_K acts on $T_l(A) = \varprojlim_n A(\overline{K})[l^n]$ the Tate module and on $V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, then we define the Galois representation attached to A as*

$$\rho_A: \; G_K \to Aut_{\mathbb{Q}_l}(V_l(\overline{K})) \simeq GL_{2g}(\mathbb{Q}_l)$$

Observation 3.10.3. *Since every elliptic cuve is an abelian variety, we will obtain Galois representations associated to elliptic curves. Then, we can obtain the explicit expressions of its Frobenius polynomials in terms of the ideals of the field where E has good reduction.*

Theorem 3.10.4. *Let $k \geq 2$, $N \geq 1$, l a prime not dividing N and $\epsilon: \; (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ a character. Then, to any normalized eigenform $f \in S_k(N, \epsilon)$, one can attach a Galois representation*

$$\rho_f: \; Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(\overline{\mathbb{Q}}_p)$$

such that

1. *ρ_f is irreducible.*

2. *ρ_f is odd.*

3. *for all primes $p \nmid Nl$, the representation ρ_f is unramified at p and*

$$\Phi_p(\rho_f)(X) = X^2 - a_p(f)X + \epsilon(p)p^{k-1}$$

Observation 3.10.5. 1. *The $L-$function of an elliptic curve coincides with the $L-$function associated to the representation associated to the elliptic curve as an abelian variety. To prove this, we use the representation associated to the elliptic curve given by $H^i_{et}(E,\mathbb{Q}_l)$, and with the help of the Frobenius automorphism, we reach an equality between both $L-$functions.*

2. *Let f be a newform on $\Gamma_0(N)$, we have a $L-$function associated*

$$L(f,s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

Using tools from complex Galois representations, we obtain an equality between this $L-$function and the $L-$function attached to the representation associated to a modular form.

Now we have related the representation theory with the $L-$functions theory, there is a wide theory about this topic. In this section, we are going to focus on the meaning of the next proposition, that, give us the existence of some Galois representation whose give us information about congruences between modular forms.

Let N be a positive integer, $k\geq 2$ an integer, and $S_k(\Gamma_0(N))$. Let $f\in S_k(\Gamma_0(N))$ newform. We denote by K_f to the subfield of $\mathbb{C}$ generated by its coefficients.

Theorem 3.10.6. *There is associated to f a continuous representation*

$$\rho_{f,\lambda}:\ Gal(\overline{\mathbb{Q}}/\mathbb{Q})\to GL_2(K_{f,\lambda})$$

satisfying

1. *$\rho_{f,\lambda}$ is unramified outside λN.*
2. *For any $p\not|\lambda N$, the characeristic polynomial of $Frob_p$ acting on $\rho_{f,\lambda}$ is $X^2-a_pX+p^{k-1}$.*

Since we can obtain $L-$functions using Galois representations, some mathematicians have studied those representations in order to obtain some information about modular forms. The second part of the theorem 3.10.6 implies that if $\rho_{f,\lambda}\simeq\rho_{g,\lambda}$, then $f=g$. Also, for two different newforms f and g we can have the same $\lambda-$representations. This happens when for all but finitely many primes p we have

$$a_p(f)\equiv a_p(g)\ mod(p)$$

The study of those congruences started with the work of Hida and Ribet [24], [25], and gave a lot of relations involving the $L-$function. Searching for a criterion, Hida [24], [25] showed that f satisfies a congruence $mod\ \lambda$ with another newform g in $S_k(\Gamma_0(N))$ if and only if λ divides the ratio

$$\delta_f=\frac{L(k,Sym^2f)}{\Omega_f}$$

with Ω_f a canonical period assiciated to f. Changing the symmetric square $L-$function by the adjoint $L-$function, which has factors

$$L_p(s,ad^0f)=(1-\frac{\alpha_p}{\beta_p}p^{-s})(1-\frac{\beta_p}{\alpha_p}p^{-s})(1-p^{-s})$$

Wiles at [26], [27], defines a more precise criterion for testing those congruences. He defined the $\eta-$invariant, and in those articles shows that

$$v_\lambda(\eta_f)=v_\lambda(\delta_f)$$

This η_f is defined by looking at a localization $\mathbb{T}_\Sigma$ of the Hecke algebra. We can see this algebra as a $\mathcal{O}_\lambda-$algebra equipped with the map

$$\pi:\ \mathbb{T}_\Sigma\to\mathcal{O}_\lambda$$

corresponding to the Hecke action of f. We define the $\eta-$invariant as

$$(\eta_f) = \pi(Ann(ker\ \pi))$$

To show the result of Wiles, he used the following theorem, which proof is in [28, lem. 4.17].

Proposition 3.10.7. *Suppose that there is a $\mathbb{T}_\Sigma-$module $\mathcal{L}$ satisfying the following properties:*

1. *$\mathcal{L}$ is finitely generated and free over $\mathcal{O}_\lambda$.*
2. *$\mathcal{L} \otimes_{\mathcal{O}_\lambda} K_\lambda$ is free of rank d over $\mathbb{T}_\Sigma \otimes_{\mathcal{O}_\lambda} K_\lambda$.*
3. *$\mathcal{L}$ is equipped with a perfect $\mathcal{O}_\lambda-$bilinear pairing*

$$\langle \cdot, \cdot \rangle :\ \mathcal{L} \times \mathcal{L} \to \mathcal{O}_\lambda$$

satisfying $\langle Tx, y\rangle = \langle x, Ty\rangle$.

If we denote $\mathfrak{p} = ker(\pi)$, the module $\mathcal{L}[\mathfrak{p}]$ is free of rank d over $\mathcal{O}_\lambda$, and for any basis $(x_1, ..., x_d)$ of $\mathcal{L}[\mathfrak{p}]$, the relation

$$\eta_f^d \subseteq \mathcal{O}_\lambda det(\langle x_i, x_j\rangle)$$

holds. If $\mathcal{L}$ is free as a $\mathbb{T}_\Sigma-$module, then we have the equality above.

Besides to proof of the Wiles criterion, this proposition give us some information to face other problems. One of this approaches is the Gross-Zagier formulae.

We construct the module $\mathcal{L}$ using H^1 of a modular curve, actually is a free $\mathbb{T}_\Sigma-$module of rank 2. Taking a basis x, y of $\mathcal{L}[\mathfrak{p}]$ such that is $K-$rational, moving this problem to the Rahm cohomology, we obtain

$$(\eta_f) = (\langle x, y\rangle) = \frac{(f, f)}{\Omega_f}$$

with Ω_f the determinant of the change of basis matrix from

$$(x, x) \to (\omega_f, \overline{\omega}_f)$$

with ω_f the one-form on X associated to f. Rankin and Shimura shows

$$(f, f) = L(1, ad^0 f)$$

Using this relation we can interpret our main result as a result related with congruences, defining the Gross's formula in this context.
Then we have obtained a relation between a Peterson product, a congruence number and a canonical period. We have a corollary of our main result 3.7.1 that is of this form

$$L(f, \chi, 1) = \frac{(f, f)}{u^2\sqrt{D}}\langle c_{f,\chi}, c_{f,\chi}\rangle$$

Also, we have the same result for the product of two $L-$function 3.7.4

$$L(f, 1)L(f \otimes \epsilon_D, 1) = \frac{(f, f)}{\sqrt{D}}\langle e_{f,D}, e_{f,D}\rangle$$

Then, Gross result is a particular case of the study of those type of quotients. Soon, we will see that those type of relations are given by the relations between a modular form and its Jacquet-Langlands associated modular forms. Since f is a modular form, we can see this as an specific case of quaternionic modular form of a Shimura variety. In the case of the modular form we have created a Shimura variety with the group $M_2(\mathbb{Q})$, i.e, a modular curve. Then the next step is to examine this type of relations over a quaternionic Shimura varieties, with this approach we will obtain more information about how the congruences between modular forms work.

Let B be a indefinite quaternionic Shimura variety and X_B its Shimura variety associated. Let g an eigenform of this variety, normalized to be rational over the field of Hecke eigenvalues. We can define a canonical period Ω_g, and then a $\eta-$invariant η_g such that

$$(\eta_g) = \frac{(g,g)}{\Omega_g}$$

This result tell us that for modular forms of weight 2, we have that this $\eta-$invariant is the same as (δ_g). In genral we have

$$(\eta_g) \subseteq (\delta_g) = \frac{(g,g)}{\Omega_g}$$

In the definite case, we can normalize g so that it lies in the $\mathcal{O}-$valued functions for some order of the quaternion algebra. We can define an $\eta-$invariant, (η_g) such that

$$(\eta_g) \subseteq ((g,g))$$

We have the Jacquet-Langlands theorem 2.6.14, such that relates modular forms associated to some quaternionic Shimura varieties, determined them by requiring that the eigenvalues of the Hecke operators acting on both are equal. Then, the question will be

How the $\eta-$ invariants η_f and η_g are related when f and g are related?

Using that the Hecke algebra for B is a quotient of the one for GL_2, we have

$$(\eta_f) \subseteq (\eta_g)$$

We have a result that says that the ratio

$$\frac{(f,f)}{(g,g)} \sim_\lambda \frac{\eta_f}{\eta_g}$$

count the congruences between f and other newforms of determined levels.

In order to study those relations and how is the behaviour of the Peterson inner product with Jacquet-Langlands related modular forms, we have the following theorem, whose proof is sketched in [15, p. 9] and uses representation theory.

Theorem 3.10.8. *Let f be a modular form of weight 2 on $\Gamma_0(N)$ with N square-free. Let $\lambda \nmid 2N$ be a prime in K_f such that $\overline{\rho}_{f,\lambda}$ is irreducible. Let Σ_f be the set of primes dividing $N\infty$. Then there exists a function*

$$\begin{aligned} c:\ \Sigma_f &\to \mathbb{C} \\ v &\to c_v \end{aligned}$$

such that if B is any quaternion algebra that f admits a Jacquet-Langlands transfer to, we have that

$$(f_B, f_B) \sim_\lambda \frac{L(1, ad^0 f)}{\prod_{v\in\Sigma_B} c_v}$$

where f_B denotes a $\lambda-$adically normalized form on B corresponding to f and Σ_B is the set of places where B is ramified. Also, if q is a finite prime in Σ_f, then $c_q \in \mathcal{O}_\lambda$ and $(c_q\mathcal{O}_\lambda)$ is the largest power of the maximal ideal in $\mathcal{O}_\lambda$ such that $\rho_{f,\lambda}$ mod $(c_q\mathcal{O}_\lambda)$ is unramified at q.

This point of view has given a lot of results, and even there are some interesting conjectures

Conjecture 3.10.9 (Shimura's conjecture)**.** *There exist a function* $c: \Sigma_\infty \to \mathbb{C}^*$ *such that*

$$(f_B, f_B) \sim_{\overline{\mathbb{Q}}^*} \prod_{v \in \Sigma_\infty,\, v \notin \Sigma_B} c_v$$

for all quaternion algebra B *that* f *transfers to.*

This conjecture arise due to the study of Hilbert modular forms from the point of view of representation theory. As we did in the beginning of this chapter, we can associate a representation to our Hilbert modular form and obtain some information about our Shimura varieties to understand how those Peterson inner product varies. Michael Harris at [30] proved the Shimura conjecture under the hypothesis that *there exist at least one finite place* v *at which* π_v *is a discrete serie.* With π the automorphic representation of $GL_2(\mathbb{A}_F)$.

Following this approach, we have other conjecture, involving a $L-$function. This conjecture comes from [31]

Conjecture 3.10.10. *Let* $\Sigma(\pi)$ *denote the set of places* v *of* f *for which the local component* π_v *is a discrete serie. Then there exist a function* $c: \Sigma(\pi) \to \mathbb{C}$ *such that*

$$(f_B, f_B) \sim_\lambda \frac{L(1, ad^0\pi)}{\prod_{v \in \Sigma_B} c_v}$$

To study this sort of problems, we have more tools appart from Jacquet-Langlands. We are going to explain the idea of how the theta-correspondence works, and how can we use this theory to our main problem, the study of how the quotients vary when f varies. Although this theory is beautiful and has a lot of applications in number theory, due to the finiteness of this dissertation, we are not going to explain in detail this tool. We are going to give the main ideas, skipping some important concepts and definitions, with the aim to show that there exists other tool that has given a result about those quotients.

This theory comes from the symplectic world. Let W be a finite dimensional symplectic space over k. Due to a result of Stone and von Neumann [29, thm. 1.3], we can divide our space as

$$W = W_1 \oplus W_2$$

This division is given by an additive character ψ with an associated representation ρ_ψ. We can define the Heisemberg group associated to W as the pairs

$$\{(u, v)\ s.t\ u \in W \text{ and } v \in k\}$$

By [29, thm. 1.3] we can construct a representation of the Heisemberg group in terms of ψ, that we are going to denote by (ρ_ψ, S).

In the construction of this theory, this group plays a crucial role, for our purpose we need to know that the Stone and von Neumann theorem, [29, thm. 1.3], gives the existence of an operator $\omega_\psi(g)$ with $g \in Sp(W)$, defined on the representation (ρ_ψ, S) as

$$\rho_\psi(gw, t)\omega_\psi(g) = \omega_\psi(g)\rho_\psi(w, t) \ \ with\ (w, t) \in H(W) \tag{3.1}$$

Definition 3.10.11. We define a *theta distribution* on $\phi \in S(W_1(\mathbb{A}))$, the Schwartz–Bruhat functions, i.e, the space of locally constant compactly supported functions on $W_1(\mathbb{A})$ as

$$\Theta(\phi) = \sum_{x \in W_1(k)} \phi(x)$$

Defining $\widetilde{Sp}_\psi(W) = \{(g, \omega_\psi(g))\ s.t\ 3.1\ holds\}$, we can define the *global theta lift* of $\phi \in S(W_1(\mathbb{A}))$ with $g \in Sp(W)(k) \setminus \widetilde{Sp}(W(\mathbb{A}))$ as

$$\theta_\phi(g) = \Theta(\omega_\psi(g)\phi)$$

With those definitions we are able to state the Seesaw duality, that will allow us to prove some relations about quotients that we have studied.

Proposition 3.10.12 (Seesaw duality)**.** *Let G, G', H, $H' \in Sp(W)$. Suppose that f is a cusp form on H and f' is a cusp form on G'. Then*

$$\langle \theta_\phi(f), g\rangle_{G'} = \langle f, \overline{\theta_\phi(f')}\rangle_{H'}$$

with $\langle f_1, f_2\rangle_G = \int_{\mathbb{C}^* \ G(k)\backslash \widetilde{G}(\mathbb{A})} f_1\overline{f_2}$.

We can apply this proposition to understand better the Peterson inner product as we want. Let f be a newform, and B a quaternion algebra over $\mathbb{Q}$. Using Shimizu's theorem, [15, thm. 5.1] which is a generalization of the theta lifting in terms of automorphic representations, we can pick a Schwartz function $\phi \in S(B(\mathbb{A}))$ such that

$$\theta_\phi(f) = \alpha \cdot (f_B \times f_B)$$

with α a non zero scalar.

As in [32], we can find a function ϕ such that

$$\theta_\phi(f_B \times f_B) = (f_B, f_B) \cdot f$$

and then, using the Seesaw duality, we find that

$$\alpha = \frac{(f, f)}{(f_B, f_B)}$$

Along the bibliography we can read this theory in detail,

Bibliography

[1] *John Voight*, Quaternion algebras, 2018.

[2] *H. Jacquet and R. P. Langlands*, Automorphic forms on GL_2. Lecture notes in mathematics. Springer-Verlag, 1970.

[3] *Lassina Dembélé and John Voight*, Explicit methods for Hilbert modular forms, 2011, arXiv.

[4] *Atsusi Ichino and Kartik Prasanna*, Periods of quaternionic Shimura varieties. I. 2016, arXiv.

[5] *P.Deligne*, Travaux de Shimura. Seminaire Bourbaki, 23 éme année (1970/71), Exp. No. 389, 1971

[6] *J. S. Milne*, Introduction to Shimura varieties, 2004.

[7] *Joseph H. Silverman*, The Arithmetic of Elliptic Curves.

[8] *Benedict H. Gross*, Heights and the Special values of $L-$series, Canadian Mathematical Society, Conference Proceedings, Volume 7, 1987.

[9] *Victor Rotger*, Introduction to Shimura varieties, CRM notes, 2005.

[10] *H.Gross and Don B. Zagier*, Heegner points and derivatives of $L-$series, Inventiones mathematicae, Springer-Verlag, 1986.

[11] *Joseph H. Silverman*, Advanced Topics in the Arithmetic of Elliptic curves, Springer-Verlag, 1994.

[12] *Ash, A. Mumford, D. Rapaport, M. and Tai*, Smooth compactifications of locally symmetric varieties, Math. Sci. Press, Brookline, Mass, 1975.

[13] *Vladimir Platonov, Andrei Rapinchuk*, Algebraic groups and number theory, Academic press, INC, 1991.

[14] *J.S. Milne*, Modular functions and Modular forms.

[15] *Periods and special values of $L-$functions*, Kartik Prasanna, Arizona Winter School notes.

[16] *Kai-Wen Lan*, An example-based introduction to Shimura varieties, procedings of the ETHZ Summer School on Motives and complex multiplicarion, 2010.

[17] *Christopher Douglas Birkbeck*, On the Jacquet-Langlands correspondence for Hilbert modular forms.

[18] *David Frederick Helm*, Jacobians of Shimura curves and Jacquet-Langlands Correspondence, PhD dissertation, 1999.

[19] *Atsushi Ichino and Kartik Prasanna*, Periods of quaternionic Shimura varieties, I., arXiv, 2016.

[20] *Kenneth A.Ribet*, Congruence Relations between Modular Forms, Procedings of the International Congress of Mathematicians, August 16-24, 1983, Warszawa.

[21] *Kenneth Ireland, Michael Rosen*, A Classical Introduction to Modern Number Theory, Springer, 1982.

[22] *Fred Diamond, Jerry Shurman*, A first course in modular forms, Springer, 2005.

[23] *Gabor Wise*, Galois Representations, 2012.

[24] *Hida, Haruzo*, Congruence of cusp forms and special values of their zeta functions. Invent. Math. 63 (1981), no. 2, 225261.

[25] *Hida, Haruzo*, On congruence divisors of cusp forms and special values of their zeta functions. Invent. Math. 63 (1981), no. 2, 221262.

[26] *Taylor, Richard; Wiles, Andrew*, Ring-theoretic properties of certains Hecke algebras. Ann. of Math (2) 141 (1995), no.3, 553572.

[27] *Wiles, Andrew*, Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) 141 (1995), no. 3, 443551.

[28] *Darmon, Henri; Diamond, Fred; Taylor, Richard*, Fermat's last theorem. Elliptic curves, modular forms and Fermat's last theorem (Hong-Kong, 1993), 214, Int. Press, Cambrigde, MA, 1997.

[29] *Prasad, Dipendra*, Weil representation, Howe duality, and the theta correspondence. Theta functions: from the classical to the modern, 105127, CRM Proc. Lecture Notes, 1, Amer. Math. Soc., Providence, RI, 1993.

[30] *Harris, Michael*, $L-$functions of 2×2 unitary groups and factorization of periods of Hilbert modular forms. J. Amer. Math. Soc. 6 (1993), no. 3 637-719.

[31] *Prasanna, Kartik*, Arithmetic aspects of the theta correspondence and periods of modular forms. Eisenstein series and applications, 251269, Progr. Math., 258, Birkhuser Boston, Boston, MA, 2008.

[32] *Thomas C.Watson*, Rankin triple products and quantum chaos. arXiv.org:0810.0425, 2008.

[33] *J.J. Duistermaat and J.A.C Kolk*, Lie groups. Universitext. Springer Verlag. First edition, 2000